

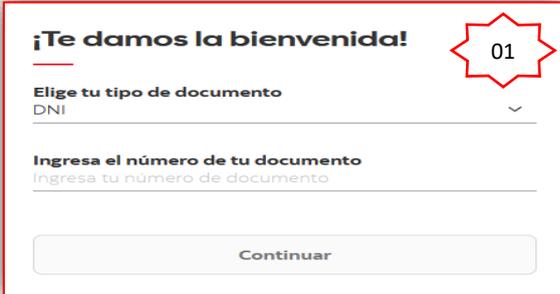
	<b>ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°210</b>		<b>Fecha: 06-09-2023</b>
			<b>Página: 10 de 13</b>
Componente que reporta	<b>DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ</b>		
Nombre de la alerta	Phishing, suplantando la identidad de la entidad Bancaria Scotiabank		
Tipo de Ataque	Phishing	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

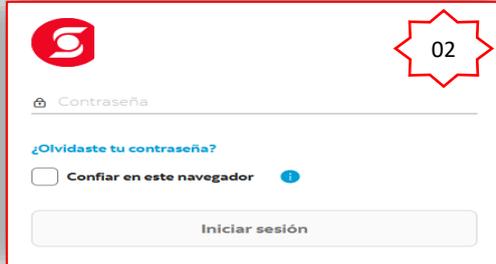
Ingresa el número de tu documento  
Ingresa tu número de documento

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.



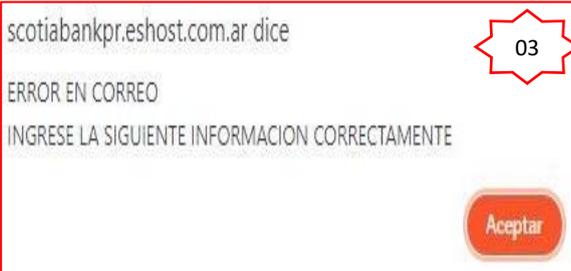
Contraseña

¿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 de continuar, 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 al sitio oficial del sitio web de Scotiabank, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturados por los cibercriminales.



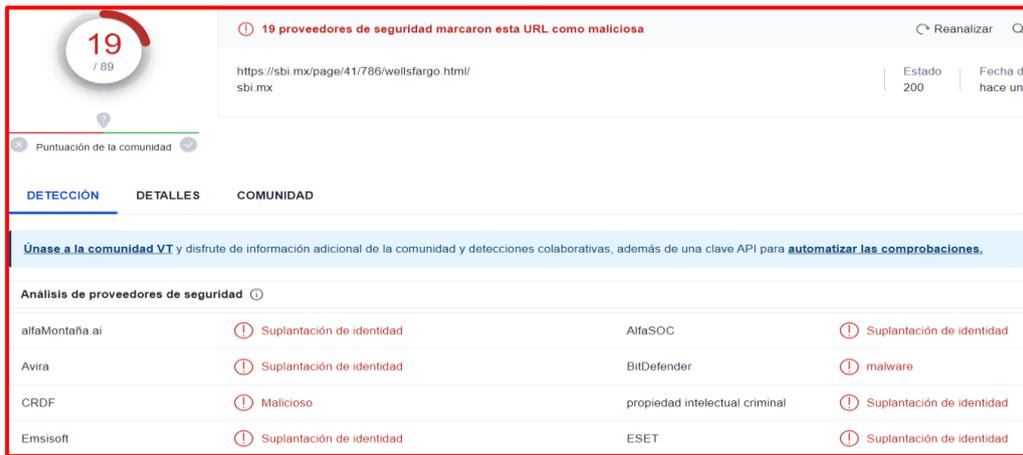
Scotiabank

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)**:



19 / 89

19 proveedores de seguridad marcaron esta URL como maliciosa

Reanalizar

Estado: 200

Fecha de actualización: hace un...

Puntuación de la comunidad

DETECCIÓN DETALLES COMUNIDAD

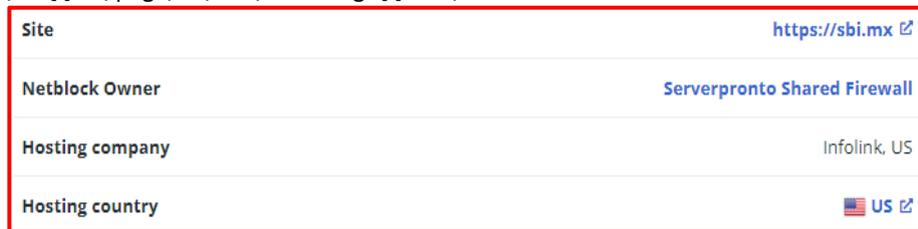
Únase a la comunidad VT y disfrute de información adicional de la comunidad y detecciones colaborativas, además de una clave API para automatizar las comprobaciones.

Análisis de proveedores de seguridad

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

• **INDICADORES DE COMPROMISO (IoC)**

- URL: `hxxps://sbi[.]mx/page/41/786/wellsfargo[.]html/`



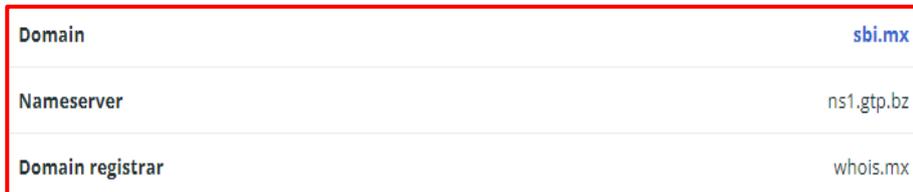
Site: <https://sbi.mx>

Netblock Owner: Serverpronto Shared Firewall

Hosting company: Infolink, US

Hosting country: US

- Dominio: `sbi.mx`



Domain: [sbi.mx](https://sbi.mx)

Nameserver: ns1.gtp.bz

Domain registrar: whois.mx

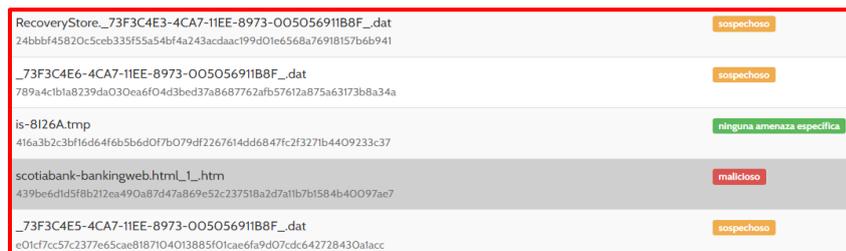
- IP: `64[.]251[.]8[.]144`



IPv4 address (64.251.8.144)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPv4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
64.0.0.0-64.255.255.255	United States	NET64	American Registry for Internet Numbers
64.251.0.0-64.251.31.255	United States	INFOLINK-BLK-100	Infolink Global Corporation
64.251.8.0-64.251.8.255	United States	INMM-64-251-8-0	Serverpronto Shared Firewall
64.251.8.144	United States	INMM-64-251-8-0	Serverpronto Shared Firewall

- SHA-256: `439be6d1d5f8b212ea490a87d47a869e52c237518a2d7a11b7b1584b40097ae7`



RecoveryStore\_73F3C4E3-4CA7-11EE-8973-005056911B8F\_dat  
24bbb45820c5ceb335f55a54bf4a243acdaac199d01e6568a76918157b6b941

\_73F3C4E6-4CA7-11EE-8973-005056911B8F\_dat  
789a4c1ba8239da030ea6f04d3bed37a8687762afb57612a875a63173b8a34a

is-8126A.tmp  
416a3b2c3b16d64f6b5b6d0f7b079df2267614dd6847fc2f3271b4409233c37

scotiabank-bankingweb.html\_1\_hm  
439be6d1d5f8b212ea490a87d47a869e52c237518a2d7a11b7b1584b40097ae7

\_73F3C4E5-4CA7-11EE-8973-005056911B8F\_dat  
e01cf7cc57c2377e65cae8187104013885f01caef9a9d07cd642728430atacc

Threat types: sospechoso, ninguna amenaza específica, malicioso, sospechoso

- Servidor: Apache

- Tipo: Text/Html

**B. Otras detenciones:**

**MALICIOSO**

 <https://sbi.mx/page/41/786/well...>

**Analizado en:** 06/09/2023 13:19:32 (...)

**Ambiente:** Windows 7 de 32 bits

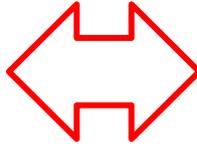
**Puntuación de amenaza:** 100/100

**Detección AV:** 20% sitio de phishing

**Indicadores:** 2 5 14

**Red:** 





**malicioso**

**Puntuación de amenaza: 100/100**

**#suplantación de identidad**

**C. Apreciación de la información:**

- La presente campaña de Phishing permite a los actores de amenazas obtener las credenciales de acceso a la banca por internet de los usuarios del Banco Scotiabank.
- La propagación del sitio web fraudulento se realiza mediante envíos masivos de email, adjuntando enlaces de sitios web fraudulentos con la finalidad de obtener información sensible de las víctimas; asimismo, a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram, Messenger, etc. y mensajes de textos SMS.

**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
------------------------	--