	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°266	Fecha: 07-11-2023
		Página: 10 de 13

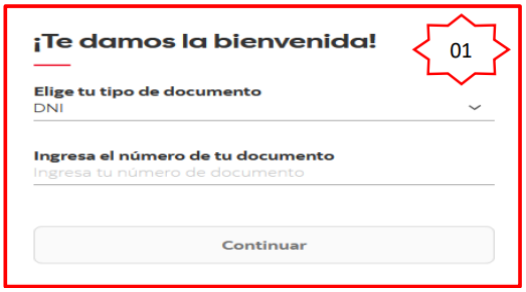
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantando la identidad de la entidad Bancaria Scotiabank		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet,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

Descripción

1. **ANTECEDENTES:**

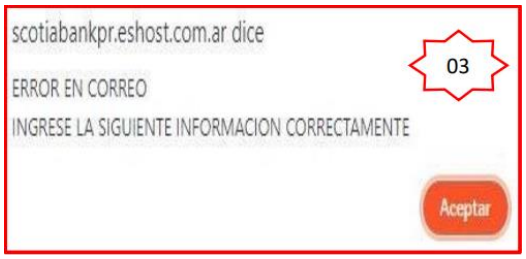
A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que actores de amenazas vienen llevando a cabo una campaña de Phishing, suplantando el sitio web del Banco Scotiabank (Banca por internet), por medio de la creación de un sitio web falso que simula el oficial, con el objetivo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

2. **DETALLES:**



Paso 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.

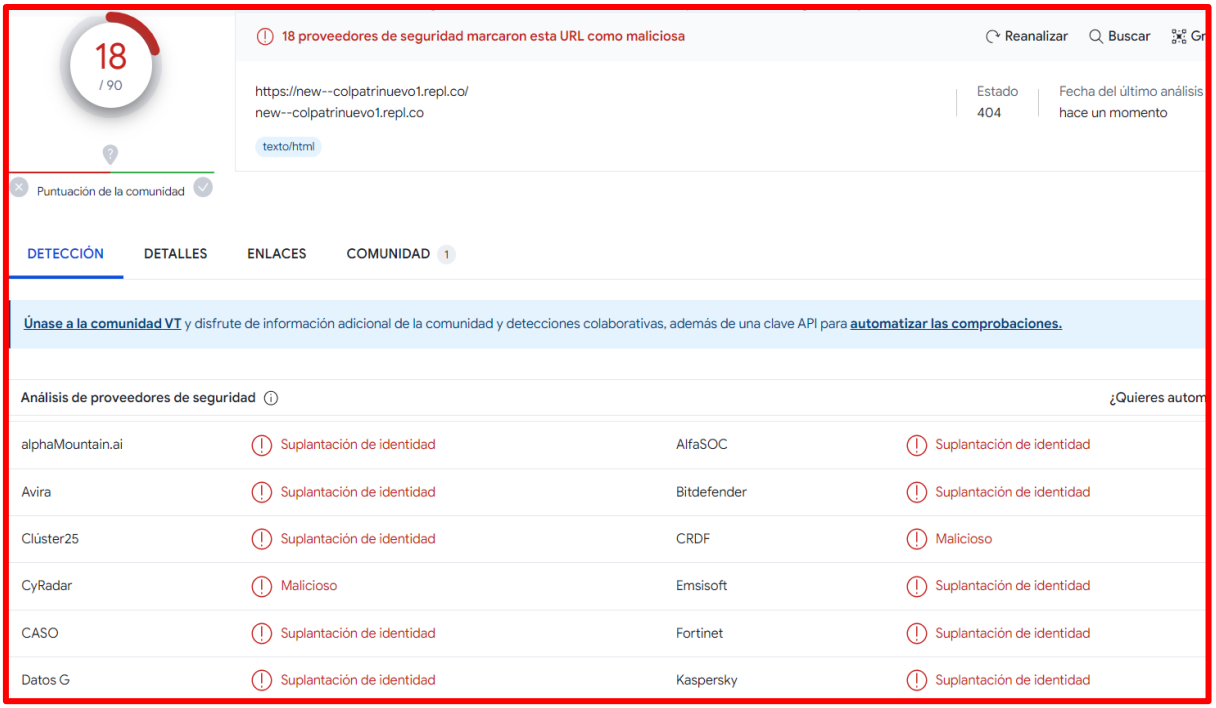
Paso 02
Luego de continuar, solicita a las víctimas ingresar la contraseña de la cuenta bancaria.



Paso 03
Después de continuar, sale una ventana emergente, en la cual informa a la víctima que ha ocurrido error al colocar el correo.

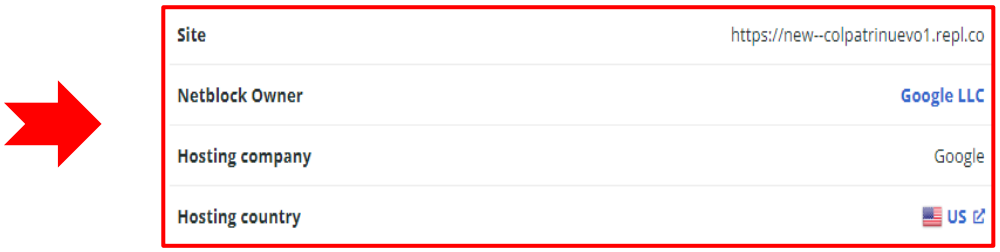
Paso 04
Finalmente, al completar lo requerido por el atacante, es redirigido al sitio oficial del sitio web de Scotiabank, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturados por los cibercriminales.

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

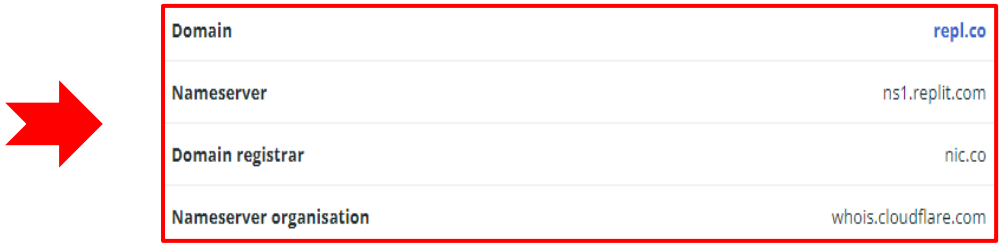


- **INDICADORES DE COMPROMISO:**

✓ **URL** : hxxps://new--colpatrinuevo1[.]repl[.]co/



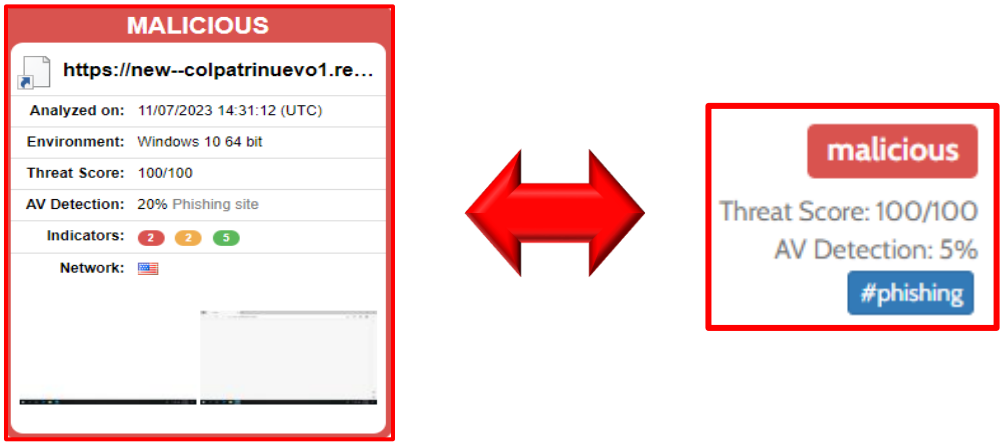
✓ **Dominio:** isn1-scotiabank[.]azurewebsites



✓ **IP** : 35[.]186[.]245[.]55

✓ **SHA-256** : f2d7708f98a8ea2376614f405f536a965820f2c696f73c913a0a413290a5cd4b

- **OTRAS DETECCIONES:**



B. Cómo funciona el Phishing:

- Los correos electrónicos incluyen enlaces de sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
- Medios de propagación del Phishing: WhatsApp, telegram, redes sociales, SMS entre otros.
- Los ciberdelincuentes intentan suplantar a una entidad legitima (organismo público o privado, entidad financiera, servicio técnico, etc.)

3. 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.

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