	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 096	Fecha: 24-04-2023
		Página 6 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 subfamilia	G02
Clasificación temática familia	Fraude		

Descripción

1. 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.

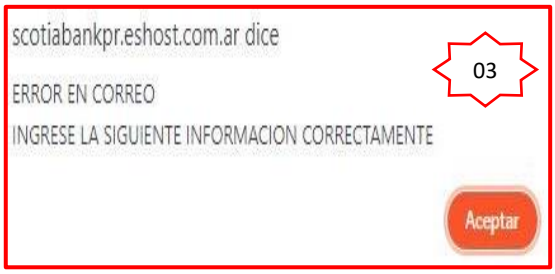
2. **Imagen**: Detalle del proceso del Phishing:

Paso N.º 01

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

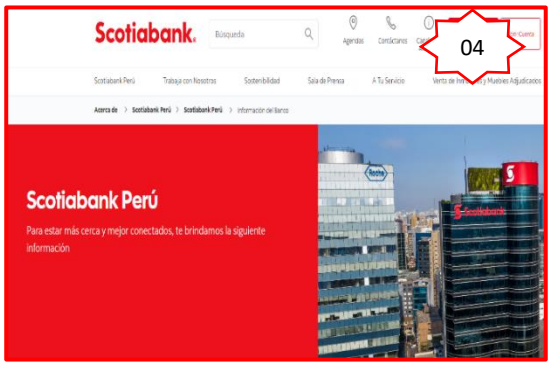
Paso N.º 02

Luego de continuar, solicita a la víctima ingresar el correo electrónico y la contraseña.



Paso N.º 03

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



Paso N.º 04

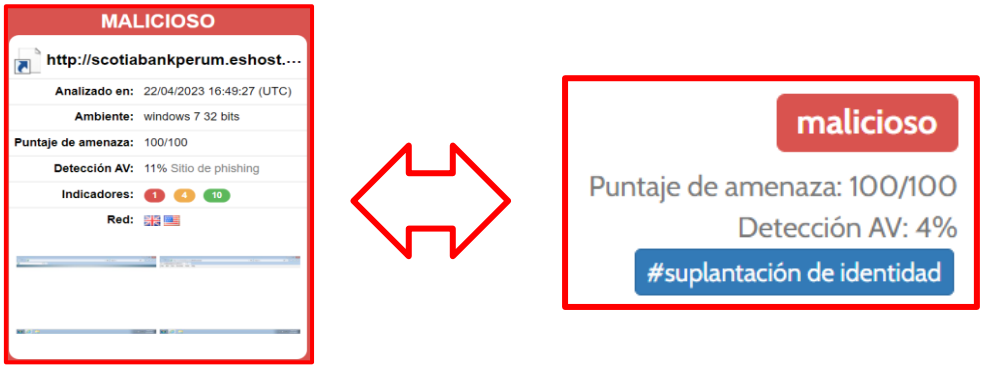
Finalmente, al completar lo requerido por el atacante, es redirigido al sitio oficial del sitio web de Scotiabank, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturados por los cibercriminales.

3. 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** : hxxp://scotiabankperum[.]eshost[.]com[.]ar/
  - **Dominio** : eshost[.]com[.]ar
  - **IP** : 185[.]27[.]134[.]155
  - **Servidor** : Nginx
  - **Tipo** : Text/Html
  - **SHA-256** : d95af03b8373743d1180e18c761aee96215cdbc5bbed768f746af72bd14cd48b

4. Otras detenciones:



5. 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 envió 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.

6. Algunas 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.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 096	Fecha: 24-04-2023
		Página 8 de 11

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Suplantación de la identidad de la red social empresarial LinkedIn		
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, quienes vienen suplantando la identidad de la red social empresarial LinkedIn, con la finalidad de obtener información confidencial de las víctimas, como dirección de correo electrónico y contraseña.

2. Imagen: Detalles del proceso de estafa del Phishing.

Sitio web falso de LinkedIn, solicita a la víctima ingresar sus credenciales de inicio de sesión (dirección de correo electrónico o número telefónico y contraseña).

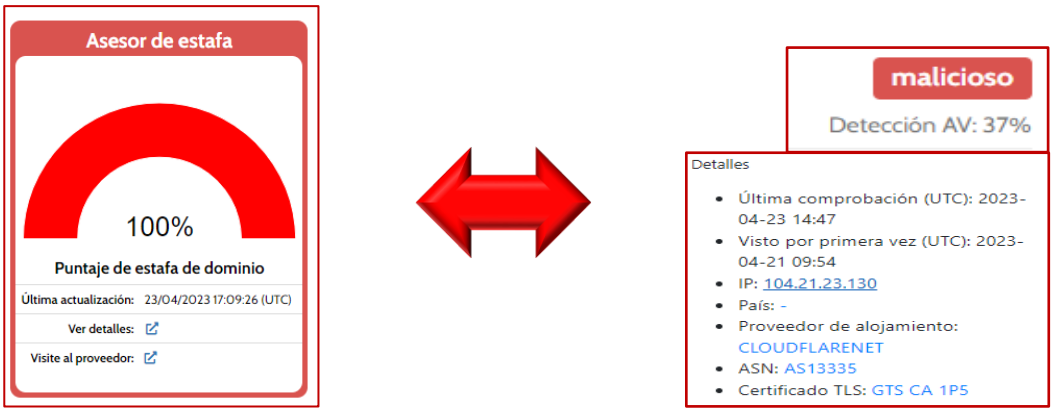
Al intentar iniciar sesión, se requiere la verificación del correo electrónico y la contraseña del e-mail; sin embargo, los datos fueron capturados por los atacantes.

3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo la siguiente información:

- **URL Malicioso:** hxxps://linkedn-id[.]cc/
- **Dominio:** linkedn-id[.]cc/
- **IP:** 104[.]21[.]23[.]130
- **Tamaño:** 46B
- **Servidor:** CLOUDFLARENET

alphaMountain.ai	Malicioso	Avira	Suplantación de identidad
CRDF	Malicioso	CyRadar	Malicioso
ESET	Suplantación de identidad	Buscador de amenazas de Forcepoint	Malicioso
Navegación segura de Google	Suplantación de identidad	kaspersky	Suplantación de identidad
Búsqueda segura	Malicioso	Sophos	Malware

- Otras detecciones del análisis:



4. Qué es LinkedIn:

- Es una plataforma para encontrar empleo o compartir tu desarrollo y crecimiento profesional. Partiendo del perfil de cada usuario, quien libremente revela su experiencia laboral además de sus destrezas, la web pone en contacto a millones de empresas y empleados.

5. Cómo funciona el Phishing:

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

6. Referencia:

- Phishing o suplantación de identidad: Es un método que los ciberdelincuentes, utilizan para engañar a los usuarios para conseguir que revele información personal, como contraseñas, datos de tarjetas de créditos, números de cuentas bancarias, entre otros.

7. Algunas Recomendaciones:

- Acceder desde fuentes oficiales a los sitios webs.
- No abrir o hacer clic en enlaces sospechosos que te lleguen por tus diferentes medios digitales.
- Proteger tu equipo con programas antivirus originales.
- No seguir instrucciones de sitios es fraudulentos es posible que infecte o se apodere tu información.
- Mantener actualizado el software de sus equipos informáticos que usas.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta