	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 072	**Fecha: 24-03-2023**
		Página 8 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección del sitio web fraudulento del Banco Interbank		
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 Interbank (Banca por internet), con la finalidad de robar información bancaria de los usuarios, como son los números de las tarjetas de crédito o débito, documento nacional de identidad (DNI), contraseñas de acceso, numero de celular, etc.

2. Detalles de proceso de Phishing del sitio web fraudulenta del Banco Interbank.

PASO N.º 01

EL ATACANTE SOLICITA A LA VÍCTIMA QUE REGISTRE EL NUMEROO DE LA TARJETA, DOCUMENTO DE IDENTIDAD Y LA CLAVE WEB DE LA BANCA POR INTERNET.

PASO N.º 02

LUEGO DE INGRESAR, EL ATACANTE INDICA QUE PARA PODER REALIZAR LAS OPERACIONES EN LA BANCA POR INTERNET ES NECESARIO VALIDAR SU TARJETA AL SISTEMA (NÚMERO DE TARJETA, OPERADOR Y NUMERO DE CELULAR, FECHA DE VENCIMIENTO, CVV Y CLAVE).

PASO N.º 03

AL VALIDAR LOS DATOS DE LA TARJETA Y DARLE CLIC EN <CONTINUAR> COMUNICA A LA VÍCTIMA QUE POSEE UNA TARJETA DE CRÉDITO Y TIENE QUE REGISTRARLO CORRECTAMENTE.

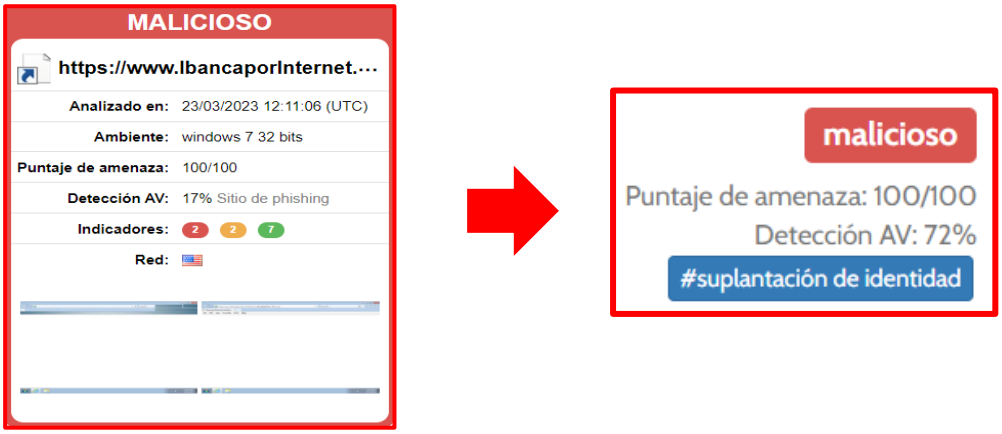
PASO N.º 04

LUEGO DE COMPLETAR TODO LO SOLICITADO POR EL ATACANTE, SEÑALA QUE ES LA PRIMERA FASE DEL PROCESO DE ACTUALIZACIÓN DE DATOS Y EN EL TRANSCURSO DE LOS DÍAS UN ASESOR SE CONTACTARÁ CON LA VÍCTIMA, SIN EMBARGO, LOS DATOS FUERON CAPTURADOS POR LOS ATACANTES.

3. La URL sospechosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultado que **QUINCE (15)** proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD - PHISHING.**

Avira	Suplantación de identidad	BitDefender	Malware
CyRadar	Malicioso	Emsisoft	Suplantación de identidad
Buscador de amenazas de Forcepoint	Suplantación de identidad	Fortinet	Suplantación de identidad
G-datos	Malware	Navegación segura de Google	Suplantación de identidad
kaspersky	Suplantación de identidad	Leonico	Suplantación de identidad
netcraft	Malicioso	OpenPhish	Suplantación de identidad
Base de datos de phishing	Suplantación de identidad	Sophos	Malware

- **URL** : hxxps://www[.]lbancaporlnternet[.]lnterbank[.]developeremir[.]com/login
- **DOMINIO:** desarrolladoremir[.]com
- **SHA-256** : b48fa7d6372e9cf775fe987608b85643dbe8804697ba36d5bc48aa471eebcc4d
- **IP** : 184[.]164[.]94[.]78
- **Tamaño** : 85.64 KB
- **OTRAS DETENCIONES**



4. Apreciación de la información:

- La presente campaña de Phishing, permite a los actores de amenazas obtener información bancaria de los usuarios del Banco Interbank

- 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.

5. 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.
- Comunicar a la entidad financiera si ha realizado un registro de acceso en un sitio web sospechoso.
- Realizar las actualizaciones correspondientes desde fuentes originales.

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