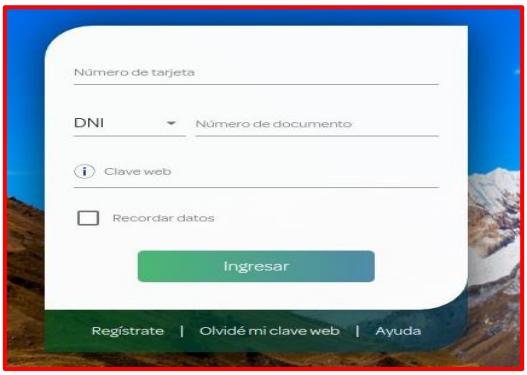
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 126	**Fecha: 30-05-2023**
		Página 7 de 10

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, número 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 número 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 número 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 llenar 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 o agente se contactará con la víctima, sin embargo, los datos ya fueron capturados por los atacantes.

3. La URL sospechosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultado que **CATORCE (14),** proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD** siendo ocho (08) y **MALICIOSO** siendo seis (06). **- PHISHING.**

alphaMountain.ai	Suplantación de identidad	AlphaSOC	Suplantación de identidad
Anti-AVL	Malicioso	Avira	Suplantación de identidad
BitDefender	Suplantación de identidad	CRDF	Malicioso
CyRadar	Malicioso	Fortinet	Suplantación de identidad
G-datos	Suplantación de identidad	kaspersky	Suplantación de identidad
Búsqueda segura	Malicioso	Sophos	Suplantación de identidad
VIPRE	Malicioso	raíz web	Malicioso

4. Indicadores de compromiso:

a) URL: hxxps://www[.]www[.]Interbank[.]benefitpe[.]com

Sitio	http://www.wwww.Interbank.benefitpe.com
Propietario de bloque de red	WEBSITEWELCOME.COM
Compañía anfitriona	Digital nuevo
país anfitrión	A NOSOTROS

b) DOMINIO: desarrolladoremir[.]com

	Prueba
✖	Registro DMARC publicado
✖	Registro DNS publicado
!	Política DMARC no habilitada

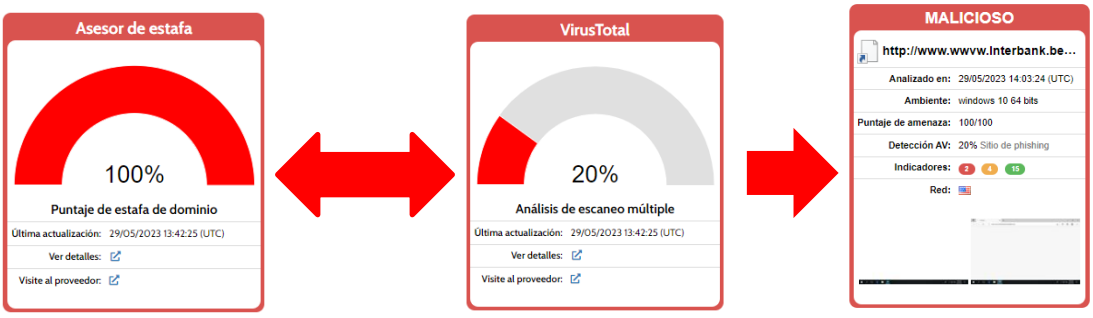
c) PROVEEDOR DE ALOJAMIENTO: ns6447.hostgator.com

Nombre del servidor	ns6447.hostgator.com
registrador de dominio	launchpad.com
Organización del servidor de nombres	whois.enom.com
Organización	Ninguno, Calle pantoja #222, Iquitos, 16003, Perú
administrador de DNS	root@gator3224.hostgator.com

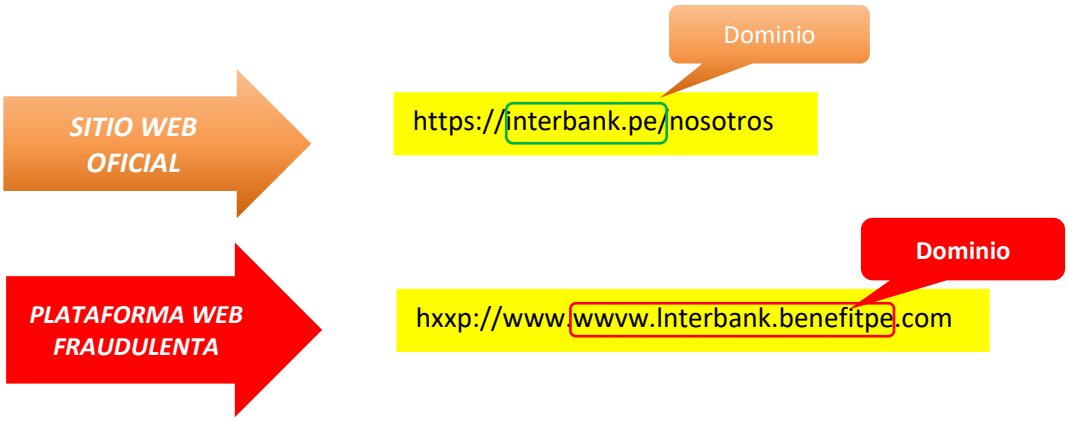
d) IP: 192[.]254[.]233[.]182

- Última comprobación (UTC): 2023-05-29 10:59
- Visto por primera vez (UTC): 2023-05-25 04:33
- IP: 192.254.233.182
- País: Estados Unidos

5. OTRAS DETECCIONES:



6. Comparación del sitio web oficial y fraudulento.



- ✓ Existe una diferencia debido a que el dominio de sitio web fraudulento no coincide con el oficial.
- ✓ Ambos sitios webs, poseen el PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS), lo que hace más convincente a que las víctimas accedan a dicho sitio web.

7. Cómo funciona el Phishing:

- Los correos electrónicos incluyen enlaces a 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.)

8. Referencia:

- 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.

9. Algunas Recomendaciones:

- Verificar detalladamente las URL de los sitios web
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio de entidades financieras 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