

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°022		Fecha: 25-01-2024
			Página: 9 de 12
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Detección de 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 Sub familia	G01
Clasificación temática familia	Fraude		

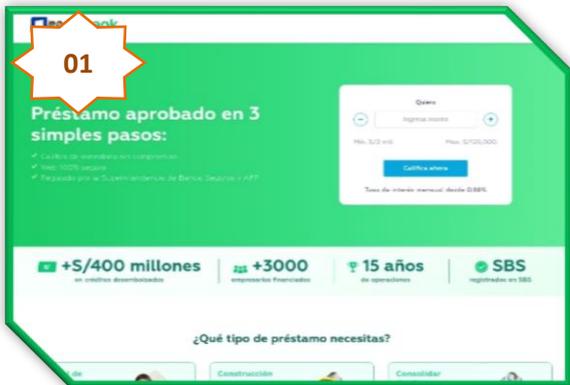
Descripción

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 de solicitud de préstamos del Banco Interbank, con la finalidad de robar información sensible de los usuarios de la entidad financiera como números de documento de identidad, tarjetas bancarias, etc.

2. DETALLES:

El proceso del Phishing es el siguiente:

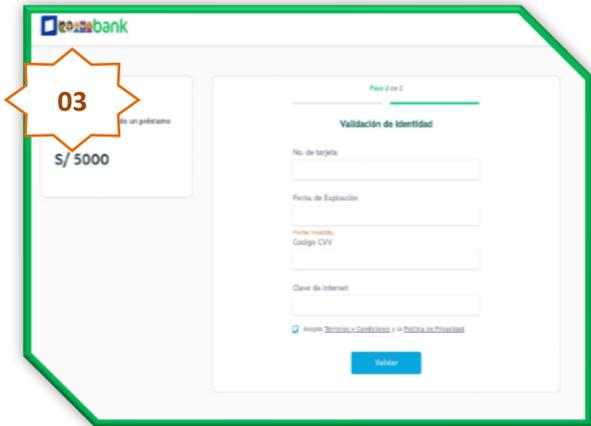
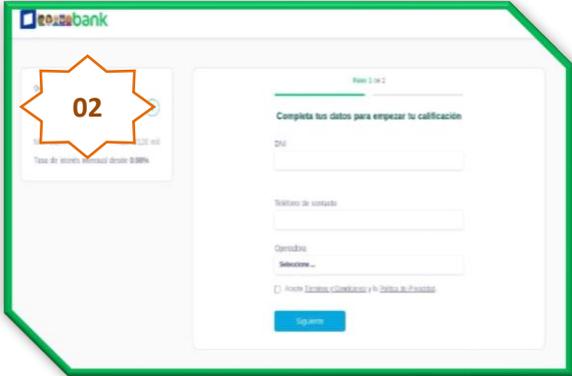


Paso N°01

Sitio web fraudulento del Banco de Interbank, solicita a la víctima registrar lo siguiente el monto del préstamo solicitado, para luego dar clic en <Calificar ahora>.

Paso N°02

Al ingresar el monto solicitado y darle clic <Calificar ahora>, solicita a la víctima completar los datos para empezar la calificación como el número del Documento Nacional de Identidad (DNI), número de celular y operador telefónico, para luego dar clic en <Siguiente>.



Paso N°03

Una vez brindado los datos solicitados en el paso N.º 02, aparece una pantalla requiriendo información como el numero de la tarjeta bancaria, la fecha de expiración, el código de seguridad (CVV) y la clave de seis dígitos del intranet, para luego dar clic en <Validar>. Pero, pasado unos segundos, redirige al sitio web oficial de la entidad bancaria; sin embargo, los ciberdelincuentes obtuvieron los datos proporcionados por la víctima.

A. Comparación del sitio web oficial y fraudulento.

SITIO WEB OFICIAL

<https://interbank.pe/solicitar/prestamo/efectivo/inicio>



Dominio: Interbank.pe

SITIO WEB FRAUDULENTA

[https://solicite\[.\]disfrutalinstante\[.\]top](https://solicite[.]disfrutalinstante[.]top)



Dominio: disfrutalinstante[.]top

- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL del sitio web fraudulento posee protocolo de seguridad de red (https)
- Existe una similitud entre ambas páginas en imagen, fondo y color.

B. Proveedor de seguridad informática no alerta como SUPLANTACIÓN DE IDENTIDAD - PHISHING.

5

/ 91

⚠️ Cinco proveedores de seguridad marcaron esta URL como maliciosa

↻ Reanalizar 🔍 Buscar 📊 Grafico 🗨 API

https://solicite.disfrutal...	Estado	Tipo de contenido	Fecha del últim...
solicita.disfrutalinstante...	200	texto/html; juego de caracteres = UTF-8	hace un moment

texto/html

DETECCIÓN | DETALLES | COMUNIDAD 13

Análisis de proveedores de seguridad ⓘ ¿Quieres automatizar c

Emsisoft	⚠️ Suplantación de identidad	Fortinet	⚠️ Suplantación de identidad
Kaspersky	⚠️ Suplantación de identidad	Netcraft	⚠️ Malicioso
Sofos	⚠️ Suplantación de identidad	Abusix	✅ Limpio

C. Indicadores de compromiso (IoC)

- Url : hXXps://solicite[.]disfrutalinstante[.]top



Site	https://solicite.disfrutalinstante.top
Netblock Owner	Cloudflare, Inc.
Hosting company	Cloudflare
Hosting country	US

- Dominio : disfrutalinstante[.]top



Domain	disfrutalinstante.top
Nameserver	bonnie.ns.cloudflare.com
Domain registrar	Unknown
Nameserver organisation	whois.cloudflare.com

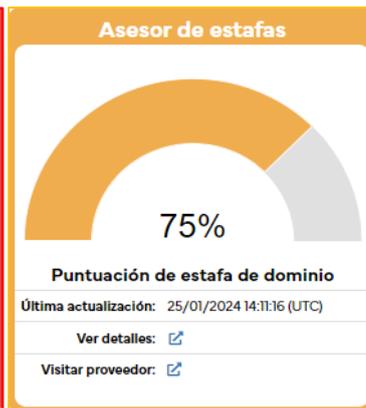
- IP : 172[.]67[.]160[.]41



IPv4 address (104.21.14.189)			
IP range	Country	Name	Description
::ffff:0:0:0:0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 104.0.0.0-104.255.255.255	United States	NET104	American Registry for Internet Numbers
↳ 104.16.0.0-104.31.255.255	United States	CLOUDFLARENET	Cloudflare, Inc.
↳ 104.21.14.189	United States	CLOUDFLARENET	Cloudflare, Inc.

- Servidor : Cloudflare
- SHA-256 : e8e9e46833d1a5d5c6437e62730ec3850b49be76ef5b1c38e41962f76bc707ff
- Tipo Contenido : Texto/Html

D. Otras detecciones



E. 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 envío 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 aceptar permisos de instalación de archivos desconocidos o dudosa procedencia.
- Mantener actualizado el sistema operativo y aplicaciones del equipo de cómputo.
- Mantener actualizado el sistema antivirus (el antivirus debe ser licenciado).
- 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.