	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°072	Fecha: 23-03-2024
		Página: 5 de 8

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:**

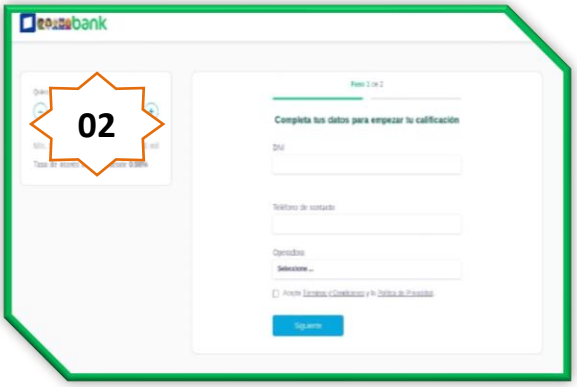
A través del monitoreo y búsqueda de amenazas en el espacio digital, se detectó que actores de amenazas vienen llevando a cabo una campaña de Phishing, suplantando el sitio web de solicitud de préstamos del Banco Interbank, con la finalidad de robar información sensible de los usuarios de la entidad financiera como números de documento de identidad, tarjetas bancarias, etc.

2. **DETALLES:**

El proceso del Phishing es el siguiente:

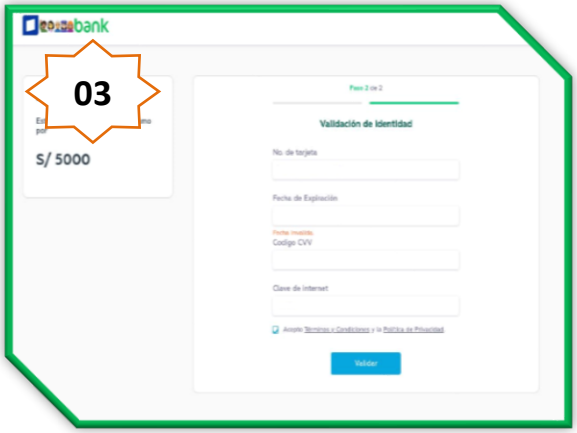
Paso Nº01

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



Paso Nº02

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>.



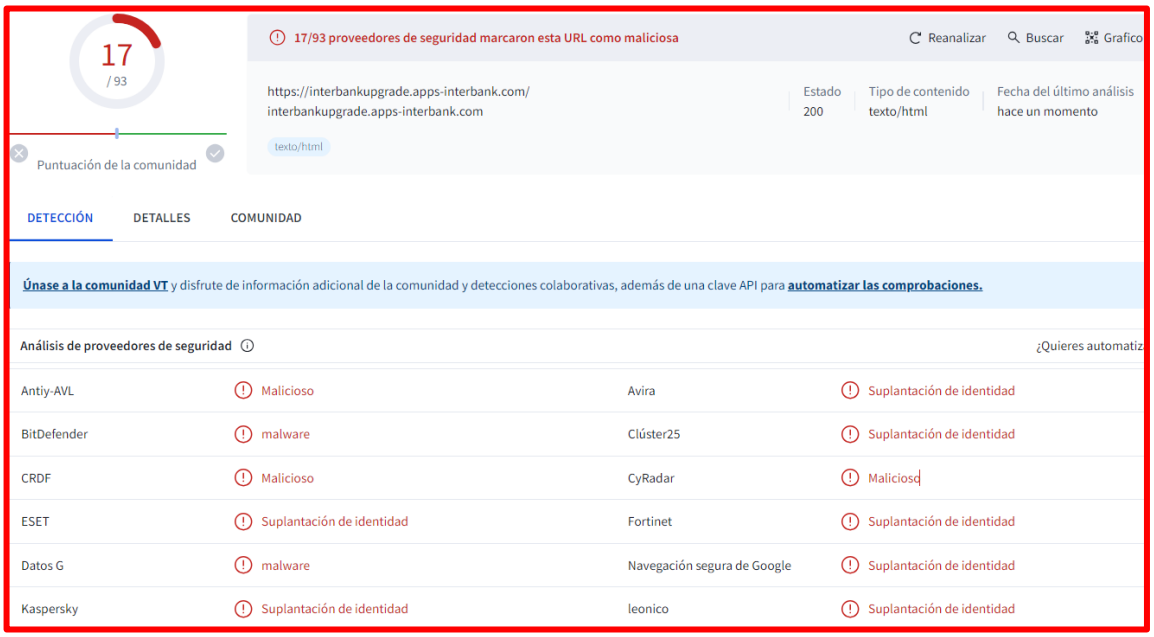
Paso Nº03

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.

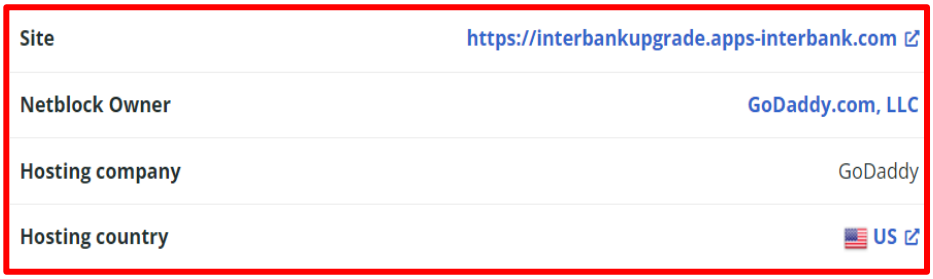
- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL del sitio web fraudulento posee protocolo de seguridad de red (https)
- Existe una similitud entre ambas páginas en imagen, fondo y color.

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

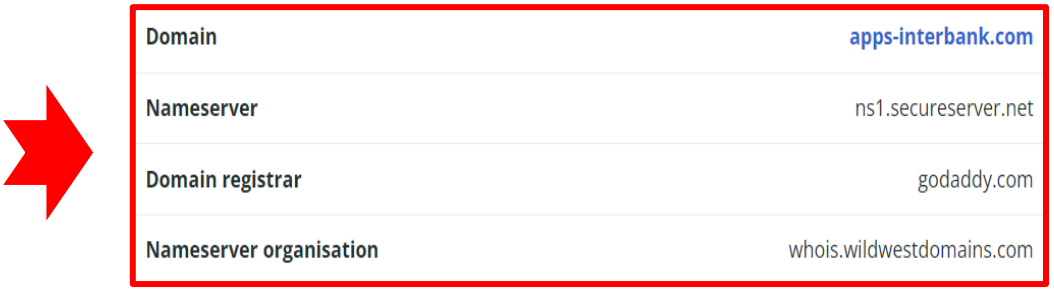


C. Indicadores de compromiso (IoC)

- Url : hxxps[:]//interbankupgrade[.]apps-interbank[.]com/



- Dominio : apps-interbank[.]com



Domain	apps-interbank.com
Nameserver	ns1.secureserver.net
Domain registrar	godaddy.com
Nameserver organisation	whois.wildwestdomains.com

- IP : 166[.]62[.]85[.]139

IPv4 address (166.62.85.139)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 166.0.0.0-166.255.255.255	United States	NET166	Various Registries (Maintained by ARIN)
↳ 166.62.0.0-166.62.127.255	United States	GO-DADDY-COM-LLC	GoDaddy.com, LLC
↳ 166.62.85.139	United States	GO-DADDY-COM-LLC	GoDaddy.com, LLC

- SHA-256 : e9bfea87b7dd52e96fc57cc17621276966a9b03828948e639042e919f016d866
- Servidor : APACHE
- Tipo Contenido : Texto/Html

D. 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.

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