

	<b>ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°301</b>		<b>Fecha: 19-12-2023</b>
			<b>Página: 11 de 14</b>
Componente que reporta	<b>DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ</b>		
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**

Requiere a la víctima ingresar al sitio web banca por internet de Interbank:

- Ingresar el número de DNI o Carnet de emergencia
- Número de celular
- Correo electrónico

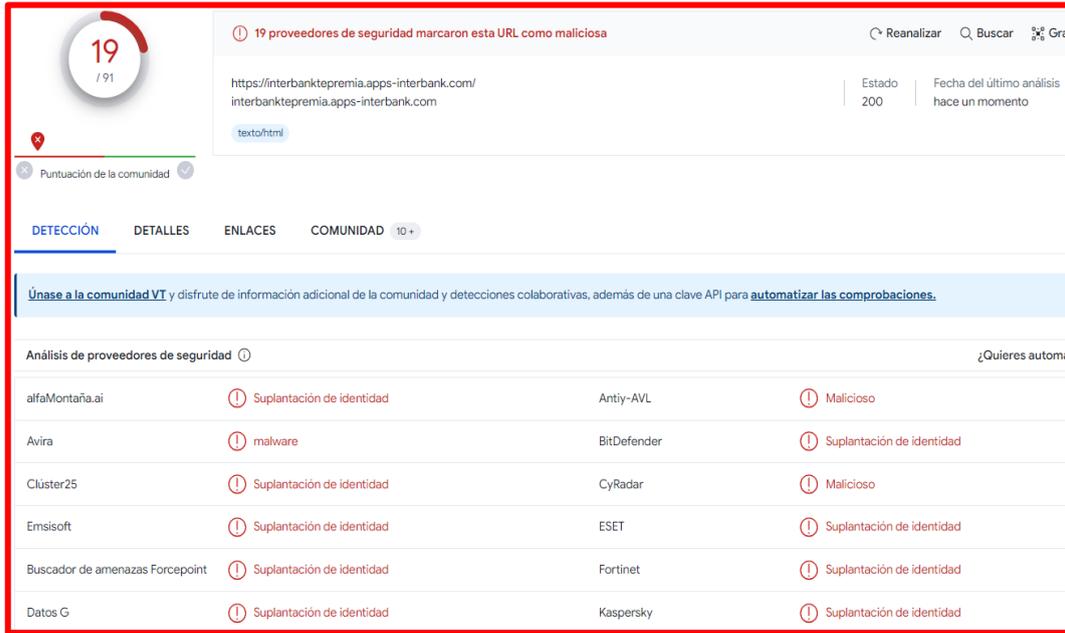
Para luego dar clic en <**QUIERO GANAR**>.



**Paso N°02**

Luego registrar sus datos, el atacante indica a la víctima que ya está participando en el sorteo; sin embargo, los ciberdelincuentes obtuvieron los datos proporcionados por la víctima.

### A. Proveedor de seguridad informática no alerta como **SUPLANTACIÓN DE IDENTIDAD - PHISHING.**



19 / 91

19 proveedores de seguridad marcaron esta URL como maliciosa

Reanalizar Buscar Gra

https://interbanktepremia.apps-interbank.com/ Estado: 200 Fecha del último análisis: hace un momento

texto/html

Puntuación de la comunidad

DETECCIÓN DETALLES ENLACES COMUNIDAD 10+

Únase a la comunidad VT y disfrute de información adicional de la comunidad y detecciones colaborativas, además de una clave API para automatizar las comprobaciones.

Análisis de proveedores de seguridad

Proveedor	Alerta	Motor	Resultado
alfaMontaña.ai	Suplantación de identidad	AntiY-AVL	Malicioso
Avira	malware	BitDefender	Suplantación de identidad
Clúster25	Suplantación de identidad	CyRadar	Malicioso
Emsisoft	Suplantación de identidad	ESET	Suplantación de identidad
Buscador de amenazas Forcepoint	Suplantación de identidad	Fortinet	Suplantación de identidad
Datos G	Suplantación de identidad	Kaspersky	Suplantación de identidad

### B. Indicadores de compromiso (IoC)

- Url : `hxpxs://interbanktepremia[.]apps-interbank[.]com/`



Site	https://interbanktepremia.apps-interbank.com
Netblock Owner	GoDaddy.com, LLC
Hosting company	GoDaddy
Hosting country	US

- 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`



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

- Servidor : Apache
- SHA-256 : 47e251f7b98408240dd95e0fa708e98d481d5c4a6d488d5219e4486b59dac56a

**C. 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.