

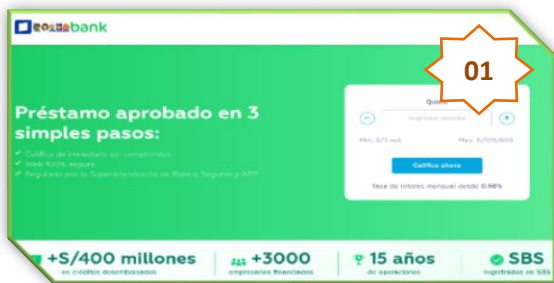
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°273		Fecha: 15-11-2023
			Página: 11 de 14
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Detección de sitio web fraudulento del Banco Interbank		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	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:

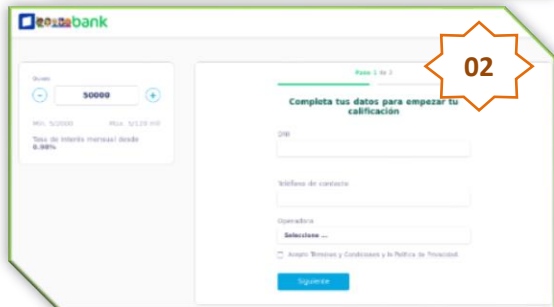


Paso N°01

Sitio web fraudulento indica a la víctima que ha recibido un préstamo en Interbank y tiene que completar en tres simples pasos:

- Ingresar el monto a solicitar

Para luego dar clic en <Calificar ahora>.

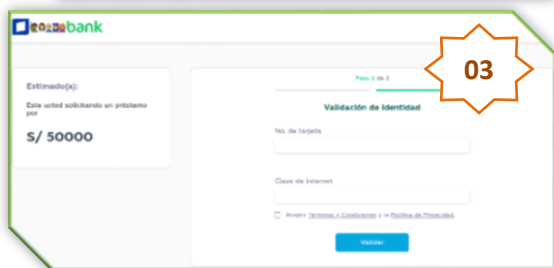


Paso N°02

Luego, solicita a la víctima datos como:

- El número de DNI
- Número de contacto
- Operador

Para luego dar clic en <siguiente>.

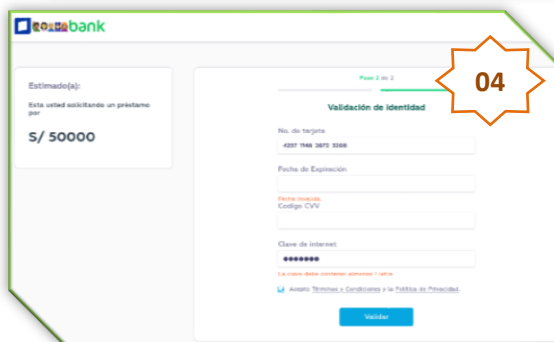


Paso N°03

Solicita a la víctima datos como:

- Número de tarjeta
- Clave de Internet

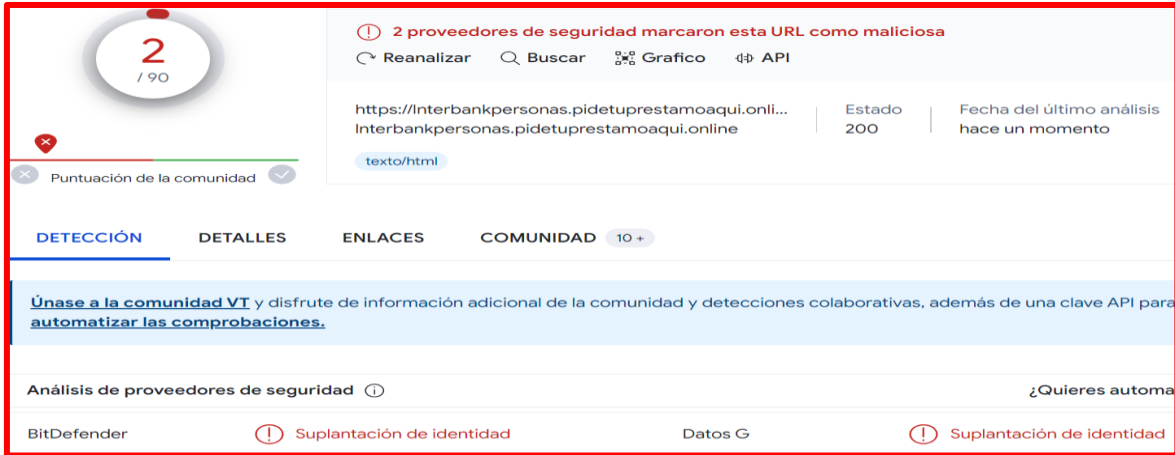
Para luego dar clic en <Continuar>.



Paso N°04

Una vez brindado los datos solicitados en el paso N.º 03, solicita fecha de expiración, el código de seguridad (CVV), 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.

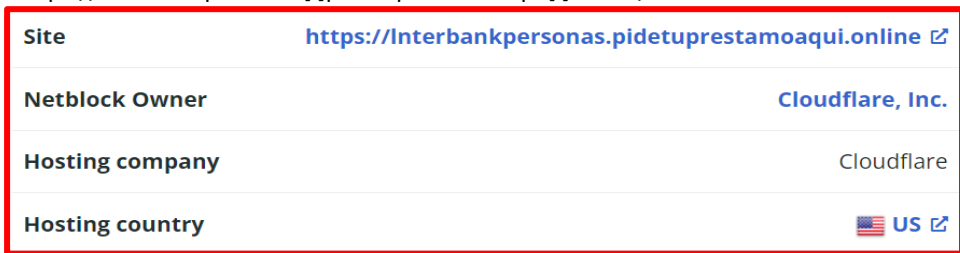
A. Proveedor de seguridad informática no alerta como SUPLANTACIÓN DE IDENTIDAD - PHISHING.



2 / 90
 2 proveedores de seguridad marcaron esta URL como maliciosa
 Reanalizar | Buscar | Grafico | API
 https://Interbankpersonas.pidetuprestamoqui.onli... Estado: 200 | Fecha del último análisis: hace un momento
 Interbankpersonas.pidetuprestamoqui.online
 texto/html
 Puntuación de la 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: ¿Quieres automa...
 BitDefender: Suplantación de identidad | Datos G | Suplantación de identidad

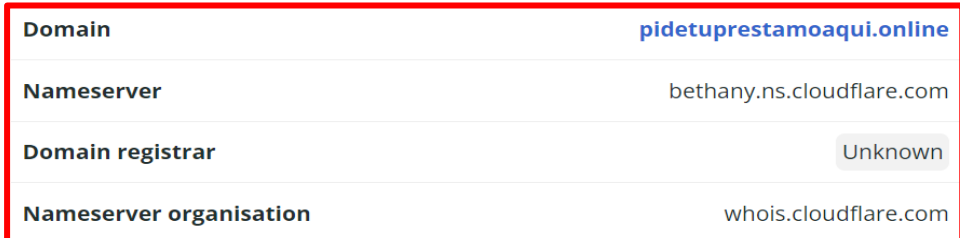
B. Indicadores de compromiso (IoC)

- Url : `hxps://Interbankpersonas[.]pidetuprestamoqui[.]online/`

Site: <https://Interbankpersonas.pidetuprestamoqui.online>
 Netblock Owner: Cloudflare, Inc.
 Hosting company: Cloudflare
 Hosting country: US

- Dominio : `pidetuprestamoqui[.]online`

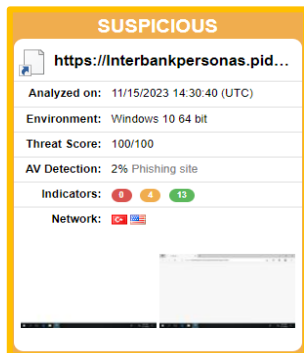
Domain: pidetuprestamoqui.online
 Nameserver: bethany.ns.cloudflare.com
 Domain registrar: Unknown
 Nameserver organisation: whois.cloudflare.com

- IP : `104[.]21[.]75[.]49`

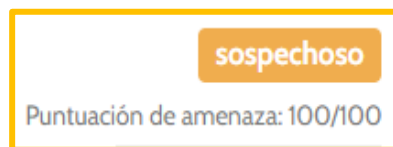



IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
104.0.0.0-104.255.255.255	United States	NET104	American Registry for Internet Numbers
104.16.0.0-104.31.255.255	United States	CLOUDFLARENET	Cloudflare, Inc.
104.21.75.149	United States	CLOUDFLARENET	Cloudflare, Inc.

- SHA-256 : `39952ad62d042fddafd62fe59224d14c2c6d451b33e4600a78f784c0ad583b42`
- Servidor : Cloudflare
- Otras detenciones



SUSPICIOUS
 https://Interbankpersonas.pid...
 Analyzed on: 11/15/2023 14:30:40 (UTC)
 Environment: Windows 10 64 bit
 Threat Score: 100/100
 AV Detection: 2% Phishing site
 Indicators: 4
 Network:

sospechoso
 Puntuación de amenaza: 100/100

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.