

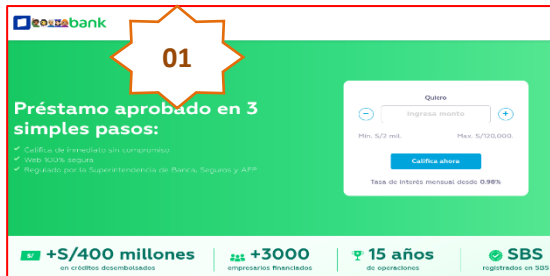
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°264		Fecha: 05-11-2023
			Página: 5 de 10
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Detección de sitio web fraudulento del Banco Interbank		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	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:

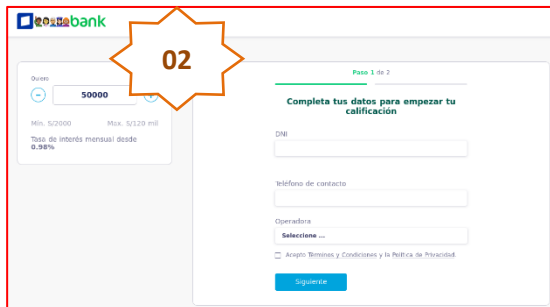


Paso N°01

Indica que Interbank brindan prestamos en tres simples pasos:

- Ingresar el monto a solicitar

Para luego dar clic en **<Calificar ahora>**.

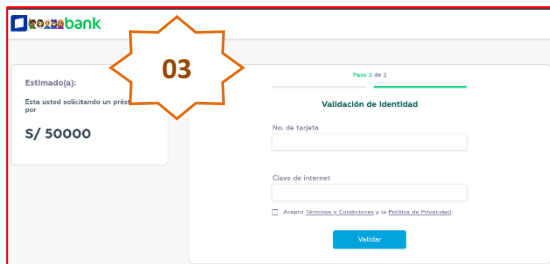


Paso N°02

Solicita a la víctima datos como:

- El número de DNI
- Número de contacto
- Operador

Para luego dar clic en **<siguiente>**.

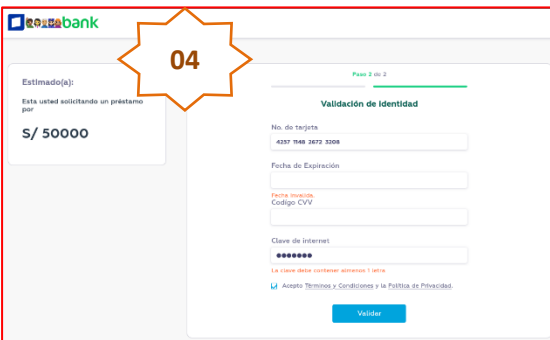


Paso N°03

Solicita a la víctima datos como:

- Número de tarjeta
- Clave de Internet

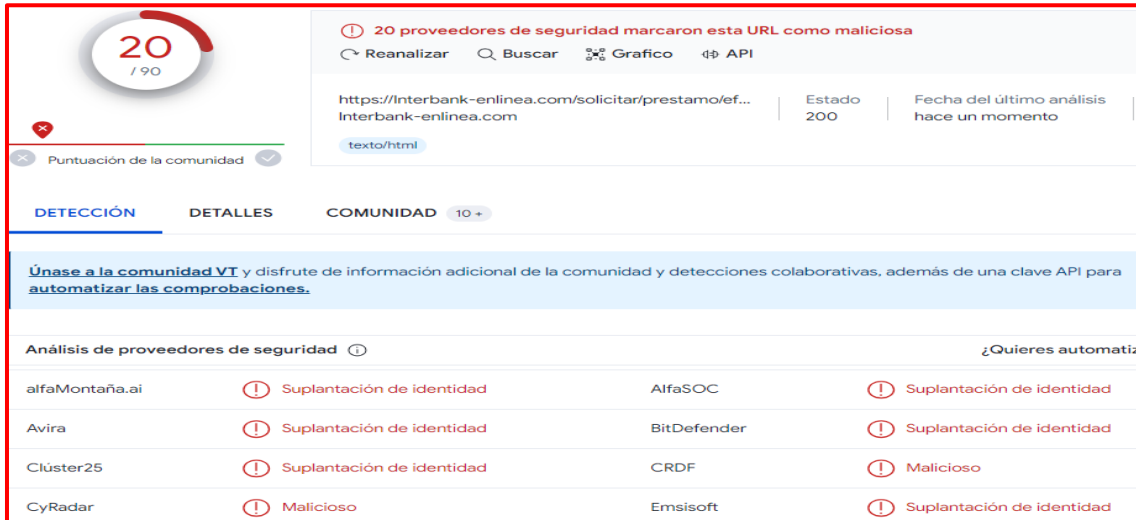
Para luego dar clic en **<Continuar>**.



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.**



20 / 90
 20 proveedores de seguridad marcaron esta URL como maliciosa
 Reanalizar | Buscar | Gráfico | API
 https://Interbank-enlinea.com/solicitar/prestamo/efectivo/ | Estado: 200 | Fecha del último análisis: hace un momento
 texto/html
 Puntuación de la comunidad:

DETECCIÓN | DETALLES | COMUNIDAD 10+

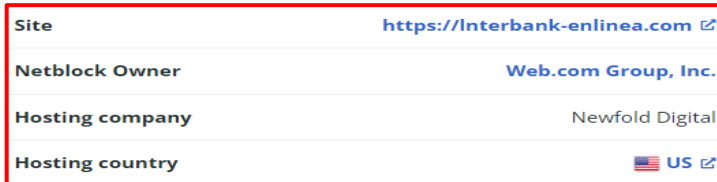
Únase a la comunidad VT y disfrute de información adicional de la comunidad y detecciones colaborativas, además de una clave API para automatizar las comprobaciones.

Análisis de proveedores de seguridad ¿Quieres automatizar?

Proveedor	Detención	Nombre	Detención
alfaMontaña.ai	Suplantación de identidad	AlfaSOC	Suplantación de identidad
Avira	Suplantación de identidad	BitDefender	Suplantación de identidad
Clúster25	Suplantación de identidad	CRDF	Malicioso
CyRadar	Malicioso	Emsisoft	Suplantación de identidad

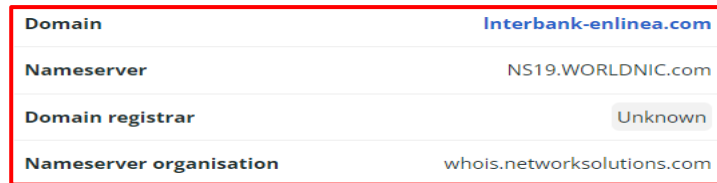
B. Indicadores de compromiso (IoC)

- Url : hxxps://Interbank-enlinea[.]com/solicitar/prestamo/efectivo/

Site <https://Interbank-enlinea.com>
Netblock Owner Web.com Group, Inc.
Hosting company Newfold Digital
Hosting country US

- Dominio : solicialo[.]top

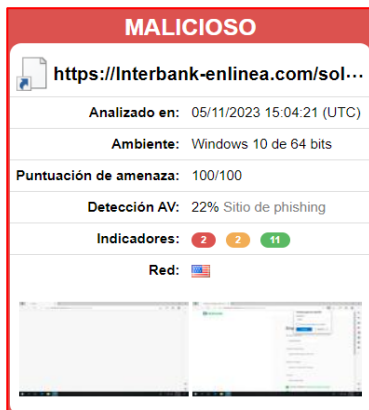
Domain Interbank-enlinea.com
Nameserver NS19.WORLDNIC.com
Domain registrar Unknown
Nameserver organisation whois.networksolutions.com

- IP : 209[.]17[.]116[.]160

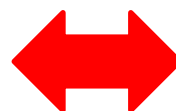
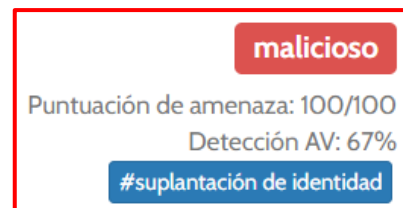



IP range	Country	Name	Description
::ffff:0:0-0:0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 209.0.0.0-209.255.255.255	United States	NET209	American Registry for Internet Numbers
↳ 209.17.112.0-209.17.117.255	United States	WEB-COM-BLK3	Web.com Group, Inc.
↳ 209.17.116.160	United States	WEB-COM-BLK3	Web.com Group, Inc.

- SHA-256 : 6665c51fa1cc9e894e0cc5ca54a4a6998ce9f47ee93a2170a80ef3ad86820ae8
- Servidor : openresty/1.19.9.1
- Tipo de cont. : Text/Html
- OTRAS DETENCIONES



MALICIOSO
<https://Interbank-enlinea.com/sol...>
 Analizado en: 05/11/2023 15:04:21 (UTC)
 Ambiente: Windows 10 de 64 bits
 Puntuación de amenaza: 100/100
 Detección AV: 22% Sitio de phishing
 Indicadores: 2 2 11
 Red:

malicioso
 Puntuación de amenaza: 100/100
 Detección AV: 67%
 #suplantación de identidad

C. 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 legítima (organismo público o privado, entidad financiera, servicio técnico, etc.)

D. Referencia:

- Phishing o suplantación de identidad: Es un método que los ciberdelincuentes, utilizan para engañar a los usuarios para conseguir que revele información personal, como contraseñas, datos de tarjetas de créditos, números de cuentas bancarias, entre otros.

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.