	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°306	Fecha: 26-12-2023
		Página: 6 de 8

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de Phishing suplantando la entidad bancaria 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:

Proceso del ciberataque:

Figura 1.
A través de un enlace el atacante le indica a la víctima que puede solicitar en el sitio web un crédito o préstamo en tres simples pasos.

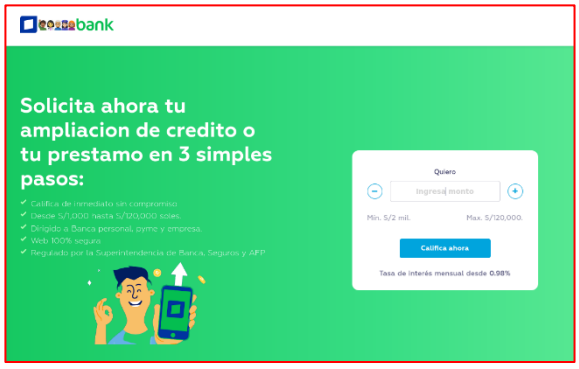


Figura 2.
Una vez ingresado el monto, requiere ingresar el DNI, Número telefónico y operador. ***Para luego hacer clic en siguiente***.

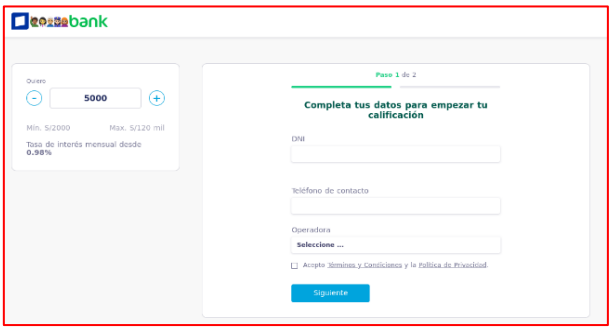


Figura 3.
Posteriormente, solicita número de tarjeta bancaria y clave o contraseña de internet. ***Para luego hacer clic en validar***.

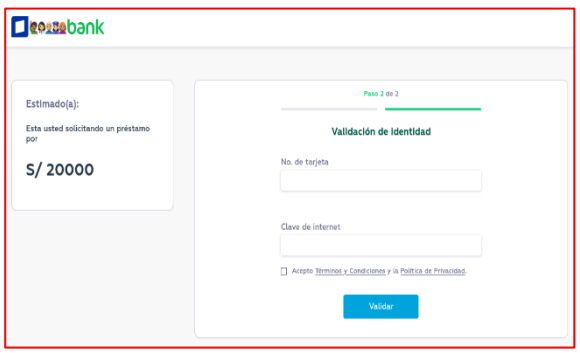
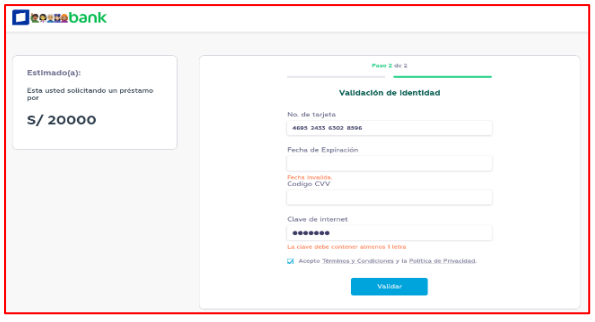


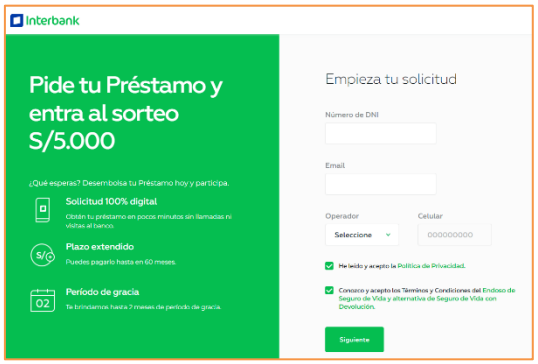
Figura 4.
Después, pide fecha de expiración de tarjeta y clave de seguridad. ***Para luego hacer clic en validar.*** Que a continuación redirige automáticamente al sitio web oficial del banco Interbank; sin embargo, los ciberdelincuentes ya obtuvieron los datos proporcionados.



A. Comparación de los sitios web legítimo y falso del Banco Interbank:

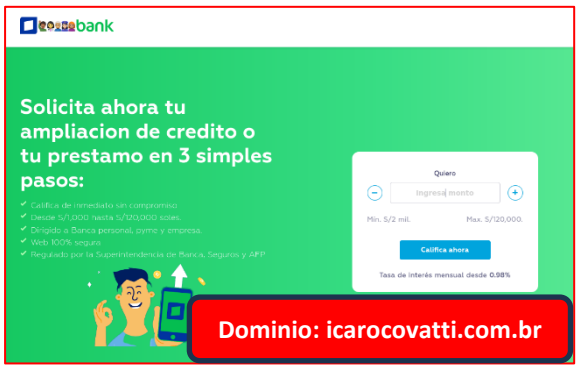
SITIO OFICIAL

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



SITIO FRAUDULENTO

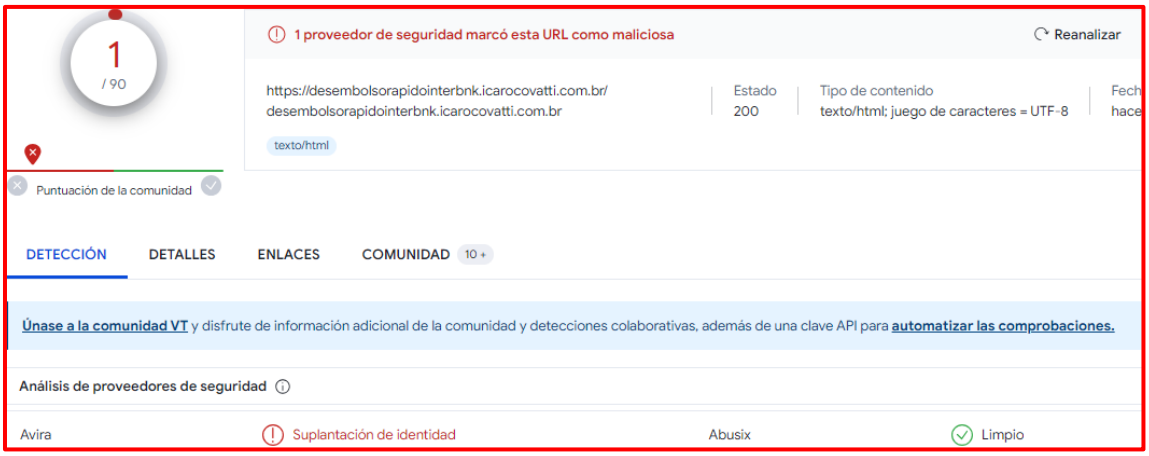
hxxps://desembolsorapidointerbnk[.]icarocovatti[.]com[.]br/



- No existe similitud entre el fondo y forma de cada sitio web.
- Existe diferente entre las URL de cada sitio web.
- El sitio web fraudulento utiliza el Protocolo seguro de transferencia de hipertexto (***HTTPS***)

B. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

- Indicadores de compromisos:
  - **Dominio:** icarocovatti[.]com[.]br
  - **Dirección IP:** 177[.]154[.]191[.]148
  - **Longitud:** 51.79 KB
  - **SHA-256**: e8e9e46833d1a5d5c6437e62730ec3850b49be76ef5b1c38e41962f76bc707ff
  - **Servidor**: Núcleo Brasil Servidores



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.