	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°300	Fecha: 18-12-2023
		Página: 8 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 Crédito del Perú		
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 realizando una campaña de Phishing, suplantando el sitio web Banca por Internet del Banco de Crédito del Perú (BCP), con la finalidad de robar información bancaria de los usuarios de la entidad financiera como números de tarjetas bancarias, clave intranet de seis dígitos, documento de identidad, correo electrónico, etc.

2. **DETALLES:**.

El proceso del Phishing es el siguiente:

Paso N.º 01

Solicitan a la víctima registrar lo siguiente:

- Número de DNI.
- Número de tarjeta.
- Clave de internet.

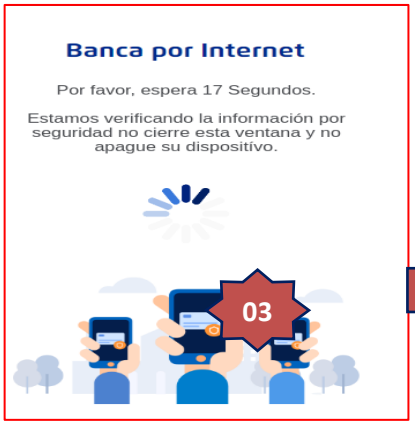
Para luego dar clic en <**Continuar**>.

Paso N.º 02

La supuesta banca por internet pide confirmar operación ingresando datos como:

- Clave digital token .

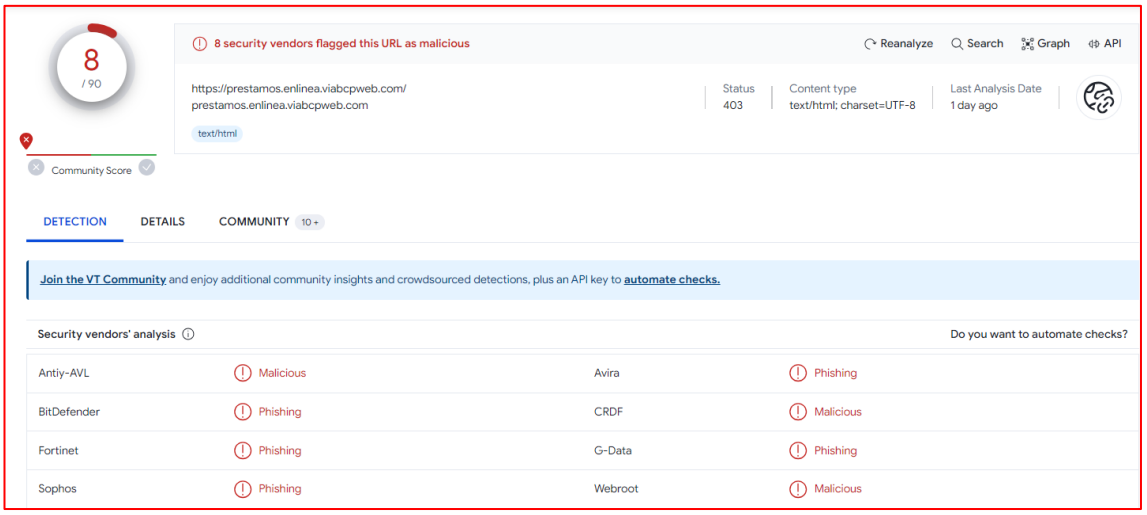
Para luego dar clic en <**Continuar**>.



Paso N.º 03

Luego, aparece una pantalla indicando que se está verificando la información ingresada, requiriendo no cerrar la ventana ni apagar el dispositivo. Redirigiendo al sitio web oficial de la entidad bancaria; sin embargo, los ciberdelincuentes obtuvieron los datos proporcionados por la víctima.

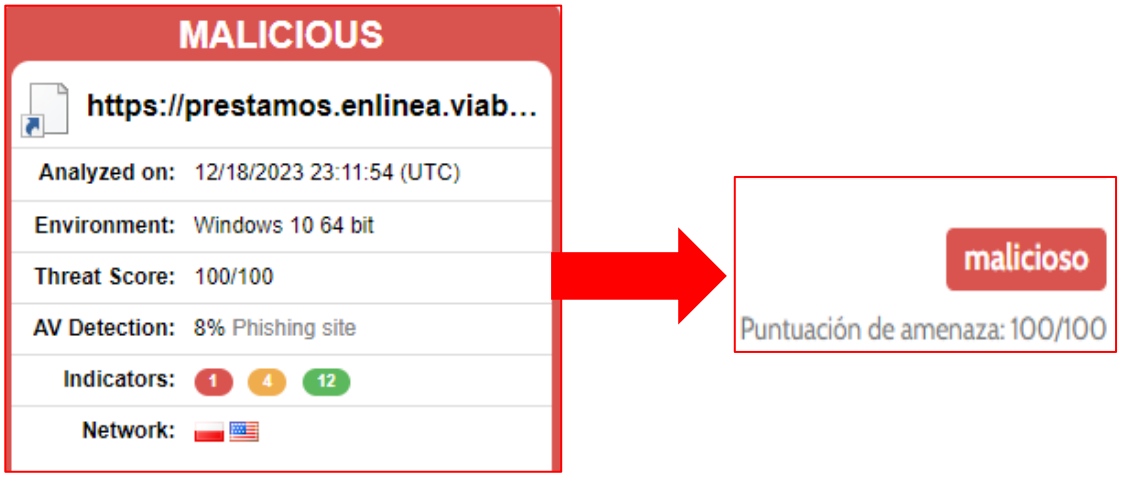
A. Proveedores de seguridad informática alertan como SUPLANTACIÓN DE IDENTIDAD - PHISHING.



B. Indicadores de compromiso (IoC)

- Dominio : prestamos[.]enlinea[.]viabcpweb[.]com
- SHA-256 : afca372f9959cb6c46bde573d25172c1b223dac52cba20ffad3c8fc2ea09cc8e
- IP : 91[.]229[.]90[.]146

C. Otras detecciones



3. RECOMENDACIONES:

- Verificar detalladamente las URL de los sitios web.
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- 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).

Fuente de Información:	Análisis propio de redes sociales y fuente abierta.