	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°181	Fecha: 03-08-2023
		Página: 10 de 13

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 llevando a cabo una campaña de Phishing, suplantando el sitio web del Banco de Crédito del Perú (servicio online de préstamo personal), con la finalidad de robar información sensible de los usuarios de la entidad financiera como números de tarjetas bancarias, clave de seis dígitos, documento de identidad, número de celular, etc.

2. **DETALLES:**

El proceso del Phishing es el siguiente:

Paso N.º 01

Solicitan a la víctima registrar lo siguiente:

- El monto solicitado del préstamo.
- Documento Nacional de identidad (DNI).
- Número de Celular.

Para luego dar clic en <Empezar>.

Paso N.º 02

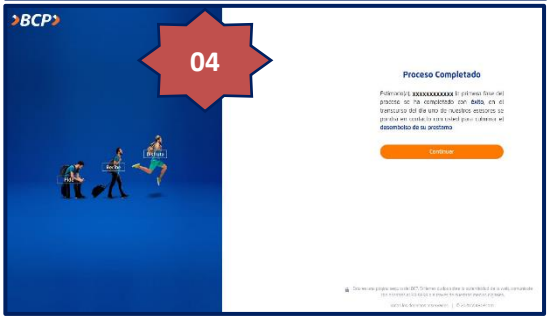
Instan a la víctima que registre datos como:

- El número de la tarjeta bancaria.
- Clave de seis dígitos (INTRANET).
- Código captcha.

Para luego dar clic en <Continuar>.

Paso N.º 03

Una vez brindado los datos solicitados en el paso N.º 02, aparece una pantalla requiriendo información de la tarjeta bancaria como la fecha de vencimiento, el código de seguridad (CVV), clave de cuatro dígitos utilizado en el cajero automático y el código captcha, para luego dar clic en <Continuar>.



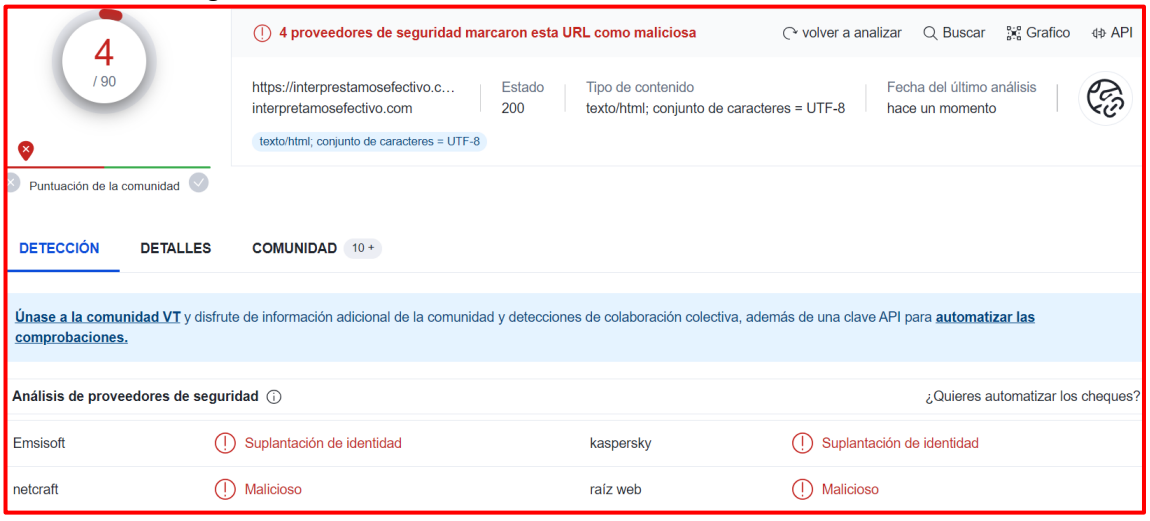
Paso N.º 04

Luego, aparece una pantalla indicando se ha completado con éxito el registro de datos y en el transcurso del día asesores de la entidad bancaria se pondrán en contacto con la víctima, para luego dar clic en <Continuar>. Redirigiendo al sitio web oficial de la entidad bancaria; sin embargo, los ciberdelincuentes obtuvieron los datos proporcionados por la víctima.

A. Comparación del sitio web oficial y fraudulento.

- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL del sitio web fraudulento posee protocolo de seguridad de red (https)
- Existe una similitud entre ambas páginas en imagen, fondo y colores de ambos sitios web.

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



C. Indicadores de compromiso (IoC)

- Dominio : interpretamosefectivo[.]com
- Servidor : LiteSpeed
- SHA-256 : eb5bc61723911fde4f515856058659393c668ddd000ec52d78206d9b2f418b23
- IP : 89[.]117[.]169[.]137

D. Otras detecciones:

E. Apreciación de la información:

- La presente campaña de Phishing permite a los actores de amenazas obtener información bancaria de los usuarios del Banco de Crédito del Perú.
- La propagación del sitio web fraudulento se realiza mediante envió 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 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).
- 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