	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°191	Fecha: 15-08-2023
		Página: 12 de 15

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Campaña de Phishing que suplanta la identidad del Banco de Crédito del Perú (BCP)		
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, los ciberdelincuentes vienen llevando a cabo ataques avanzados de Phishing, dirigidos a usuarios de la identidad del Banco de Crédito del Perú (BCP), con el objetivo robar credenciales de acceso, datos personales y bancarios.

2. **DETALLES:**

Imagen 1:
El atacante le solicita a la víctima registrar las credenciales de acceso (DNI, N.º de tarjeta y clave de internet de 6 dígitos).

Imagen 2:
Luego de ingresar las credenciales de acceso, le informa a la víctima que se está verificando la información.

Imagen 3:
Luego, le solicita a la víctima registrar la clave digital "Token" para poder ingresar a la banca por Internet.

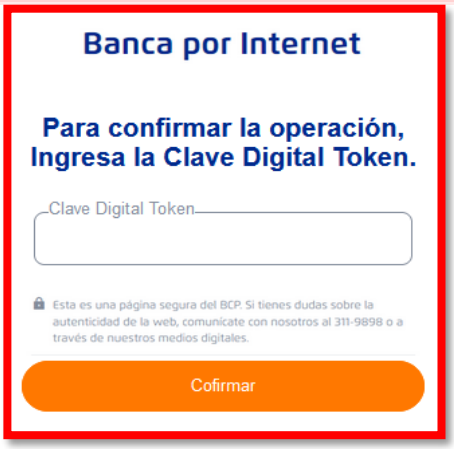
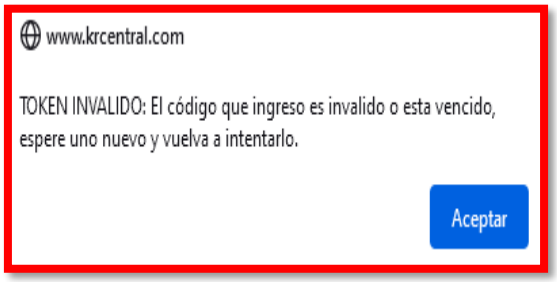
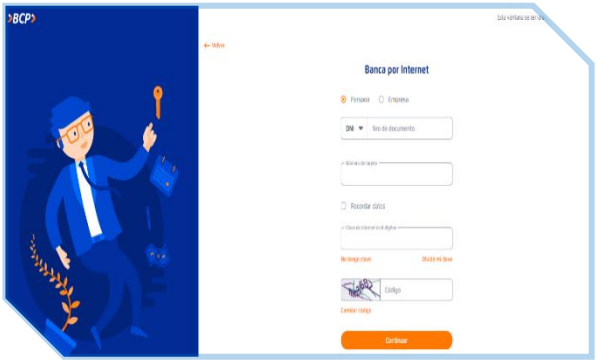


Imagen 4:
Por último, al registrar el token varias veces le informa que el código que ingreso es invalido o esta vencido; sin embargo, los ciberdelincuentes ya obtuvieron los datos proporcionados por la víctima que luego son usados para realizar operaciones sin el consentimiento del titular.



A. Comparación del sitio web oficial y sitio web falso del BCP:

SITIO WEB OFICIAL https://loginunico.viabcp.com/#/tarjeta-sesion	SITIO WEB FRAUDULENTO hxxp://www[.]krcentral[.]com/



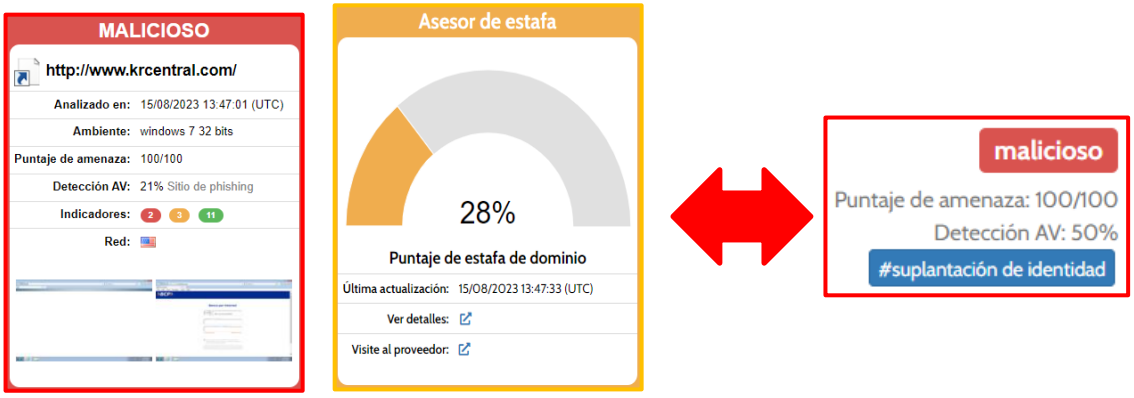
- No existe una similitud entre el fondo y forma de cada sitio web.
- Hay diferencia en el dominio, debido a que el sitio web fraudulento no coincide con el sitio oficial del BCP.
- No posee el ***PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS),*** lo que hace más convincente a las posibles víctimas que no accedan a dicho sitio web.

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

C. Indicadores de compromiso (IoC)

- URL : hxxp://www[.]krcentral[.]com/
- Dominio : krcentral[.]com
- SHA-256 : e3e9f601cc4a17d7953fc3253179b32e577fcaad49f67f0f6725c460b76850af
- IP : 204[.]93[.]178[.]122
- Servidor : Apache
- Tipo : Text/Html

D. Otras detenciones:



E. 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.

F. *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 la URL, que corresponda al sitio web oficial.
- No brindar información cuando las entidades bancarias soliciten actualización de datos confidenciales de manera online.
- Ingresar desde fuentes oficiales.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.
- Evitar compartir la URL con amigos y/o familiares.

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