	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°225	Fecha: 24-09-2023
		Página: 5 de 10

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:

Para solicitar un préstamo el atacante le solicita a la víctima registrar el número del Documento Nacional de Identidad (DNI), el monto del préstamo solicitado y el número de Celular.

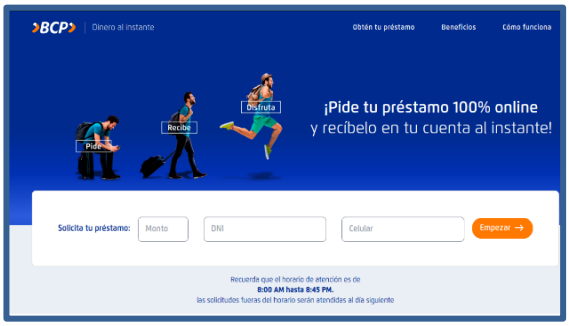


Imagen 2:

Luego de completar con lo requerido, le solicita a la víctima el número de tarjeta de crédito o débito y clave de seis dígitos (INTRANET), para luego dar clic en <Continuar>.

Imagen 3:

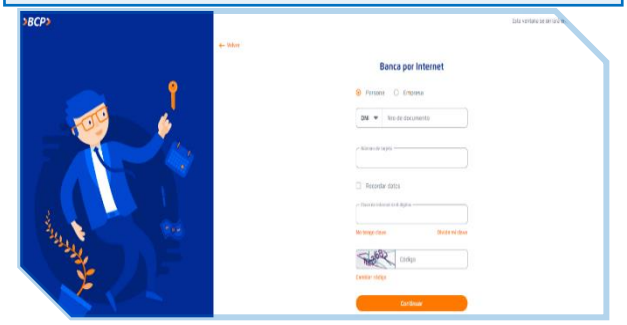
Una vez brindado los datos solicitados en el paso N.º 02, aparece una pantalla requiriendo información de la tarjeta bancaria como la fecha de vencimiento, el código de seguridad (CVV) y la clave de cuatro dígitos utilizado en el cajero automático, para luego dar clic en <Continuar>.

Imagen 4:

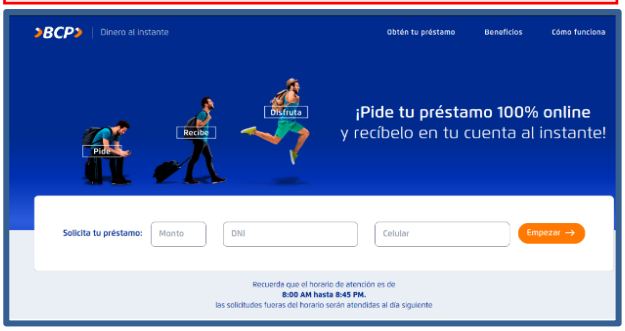
Luego, aparece una pantalla indicando que el proceso se ha completado con éxito y que un asesor de la entidad se comunicará con la víctima, para culminar con el desembolso del préstamo, para luego hacer clic en <Continuar>.

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

SITIO WEB OFICIAL
https://loginunico.viabcp.com/#/tarjeta-sesion

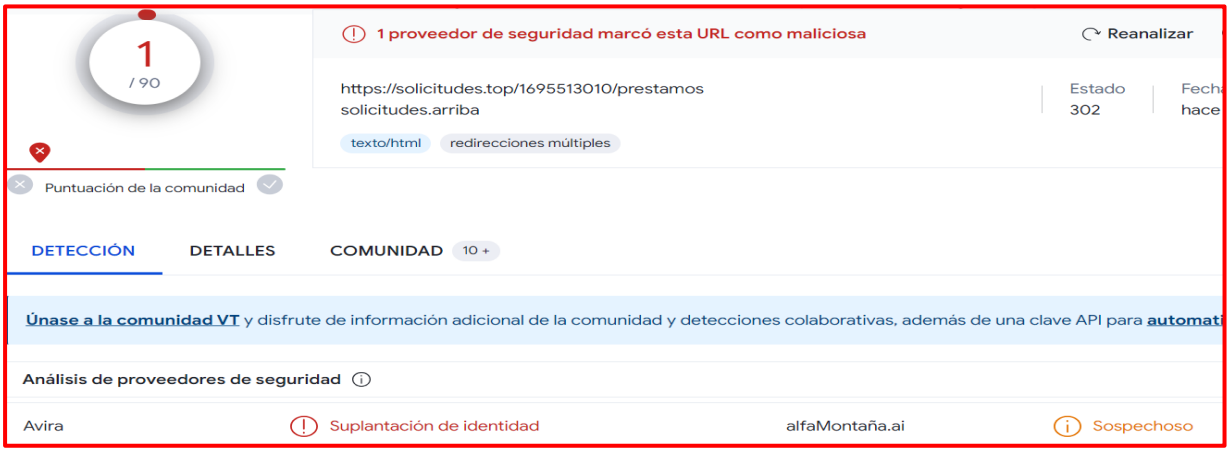


SITIO WEB FRAUDULENTO
hxxps://solicitudes[.]top/1695513010/prestamos



- 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.
- La URL posee el ***PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS),*** esto hace que la víctima registre sus datos personales en dichos sitio web.

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



C. Indicadores de compromiso (IoC)

- Dominio : solicitudes[.]top
- SHA-256 : 0bad283f8b8cf8313b26a6ca57a87fe2366a77fee12e4725da298ad67cdcb4f3
- IP : 172[.]67[.]170[.]148
- Servidor : cloudflare
- 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, ya que las entidades bancarias no solicitan 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.

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°225	Fecha: 24-09-2023
		Página: 8 de 10

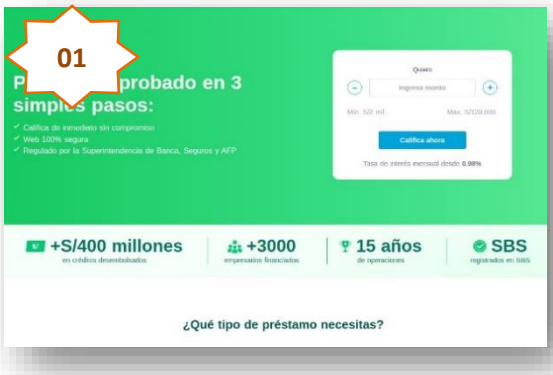
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de sitio web fraudulento del Banco Interbank		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
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:**

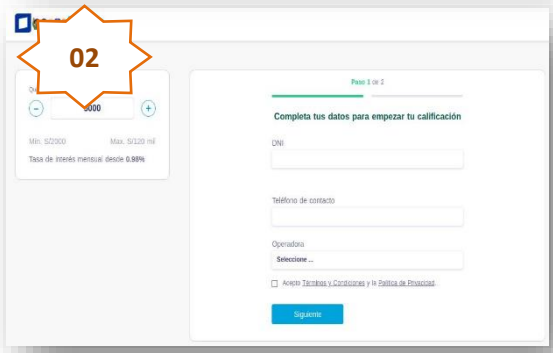


Paso Nº01

Solicitan a la víctima registrar lo siguiente:

- El monto del préstamo solicitado.

Para luego dar clic en <Calificar ahora>.

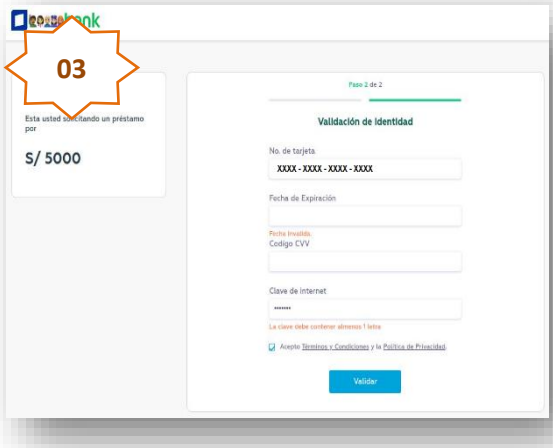


Paso Nº02

Solicita a la víctima datos como:

- El número del Documento Nacional de Identidad (DNI).
- Número de celular
- Operador telefónico

Para luego dar clic en <Siguiente>.



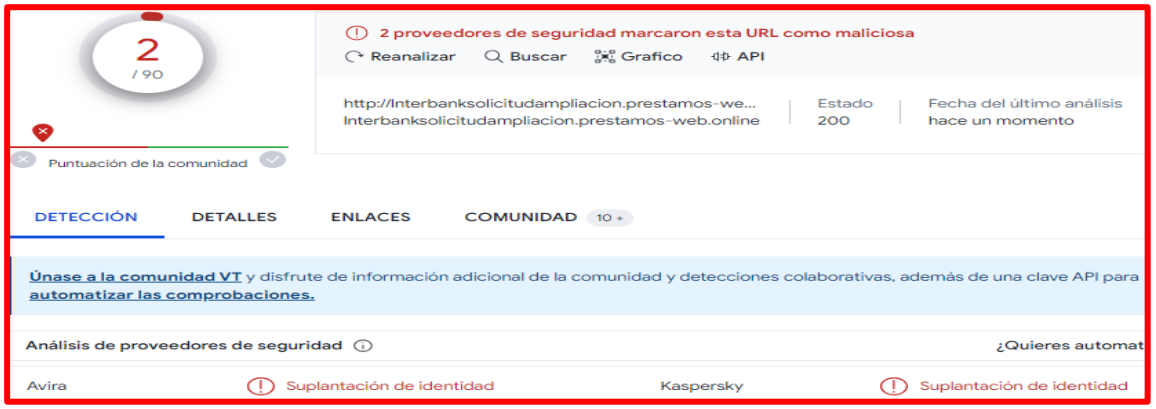
Paso Nº03

Una vez brindado los datos solicitados en el paso N.º 02, aparece una pantalla requiriendo información como el numero de la tarjeta bancaria, la fecha de expiración, el código de seguridad (CVV) y la clave de seis dígitos del intranet, 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. 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 color.

B. Proveedor de seguridad informática no alerta como SUPLANTACIÓN DE IDENTIDAD - PHISHING.



C. Indicadores de compromiso (IoC)

- Dominio : prestamos-web[.]online
- IP : 47[.]251[.]51[.]48
- Servidor : Apache
- SHA-256 : 912bb640cf3f2efca7beebe830ab4428c248fd640450a17ce01dda54e610a3e5
- Tipo Cont : Texto/Html
- Codigo : 200

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.