	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°245	Fecha: 16-10-2023
		Página: 12 de 15

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:

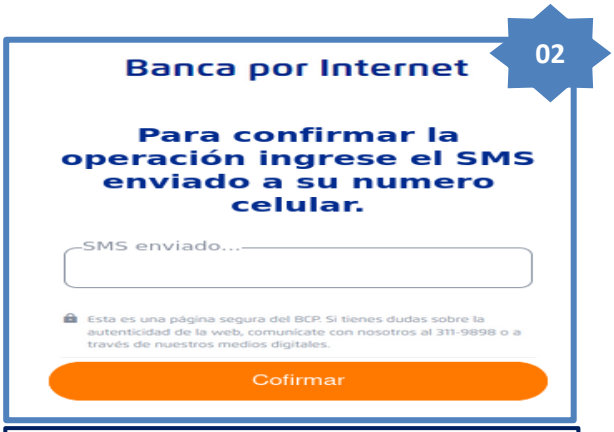
A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que actores de amenazas vienen llevando a cabo una campaña de Phishing, suplantando el sitio web del Banco de Crédito del Perú (servicio online de préstamo personal), con la finalidad de robar información sensible de los usuarios 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:

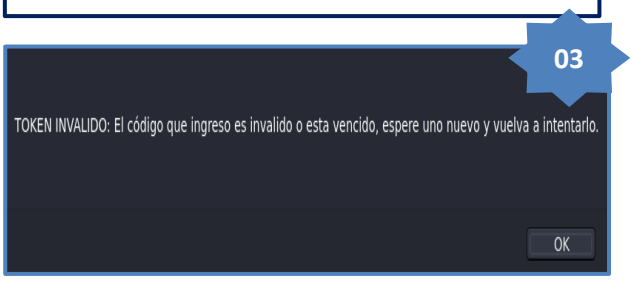
Paso N.º 01

Sitio web fraudulento solicita a la víctima registrar el numero de DNI, numero de tarjeta y la clave de internet de seis dígitos, para poder continuar e ingresar.



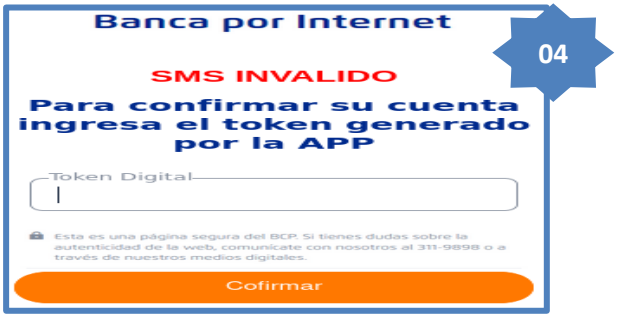
Paso N.º 02

Luego de completar lo requerido, el atacante insta a la víctima que confirme el mensaje que se le ha enviado a su número de celular, para poder continuar.



Paso N.º 03

Una vez brindado los datos solicitados en el paso N.º02, aparece una pantalla en donde se le informa que el token es invalido o esta vencido y se requiere que se vuelva a intentar, para luego dar clic en <OK>.



Paso N.º 04

Luego, indica que ingrese el token, minutos después de haber completado el registro del token el atacante le informa a la víctima que ha colocado incorrecto; 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.

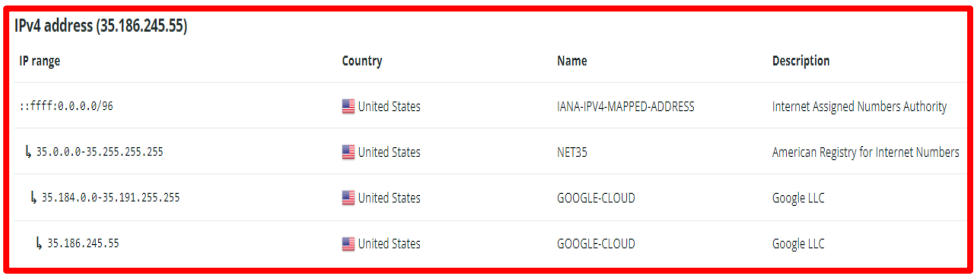
B. Proveedores de seguridad informática alertan como SUPLANTACIÓN DE IDENTIDAD - PHISHING.

C. Indicadores de compromiso (IoC)

- Dominio : repl[.]co

Domain	repl.co
Nameserver	ns1.replit.com
Domain registrar	nic.co

- IP : 35[.]186[.]245[.]55



IPv4 address (35.186.245.55)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 35.0.0.0-35.255.255.255	United States	NET35	American Registry for Internet Numbers
↳ 35.184.0.0-35.191.255.255	United States	GOOGLE-CLOUD	Google LLC
↳ 35.186.245.55	United States	GOOGLE-CLOUD	Google LLC

- Tipo de Conte. : Text/Html
- SHA-256 : ba2e3ea41c90a798d99edc791a52ae6b316f3cfb10b5e998329e67afbab19a78

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.