	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 115	Fecha: 17-05-2023
		Página 8 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Campaña de phishing suplantando 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 subfamilia	G02
Clasificación temática familia	Fraude		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de Phishing, por medio de los diferentes navegadores web, dirigido a los clientes y/o usuarios del Banco de Crédito del Perú - BCP; el cual mediante la creación de un sitio web similar al original, solicita a las posibles víctimas registrar los datos personales de la Banca por internet, registrando como el N.º DNI, N° de tarjeta bancaria, clave web, fecha de vencimiento, clave de seguridad, número de contacto, entre otros.

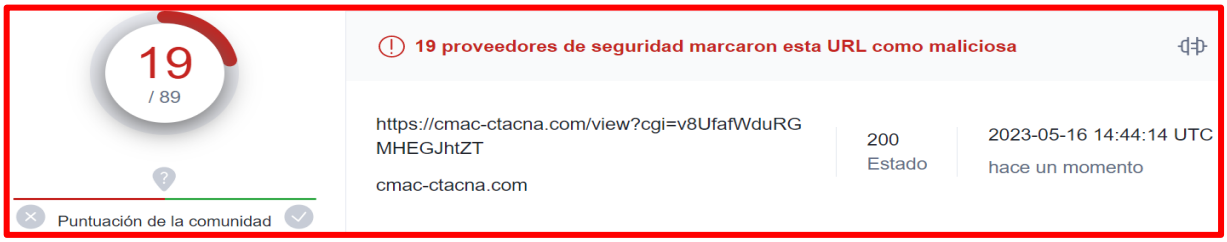
2. Proceso del ataque phishing:

El atacante solicita a las posibles víctimas a ingresar los datos personales de la Banca por Internet como es el N.º DNI, N.º Tarjeta, Clave del sitio web y código para continuar.

Luego de continuar, solicita a la víctima validar el N.º de Tarjeta como la fecha de vencimiento, código de seguridad (CVV), clave de cajero (ATM), operador de teléfono y N.º de celular.

Finalmente, al completar lo requerido por el atacante, le indica a la víctima que el proceso de validación se ha completado con éxito, luego es redirigido al sitio oficial del sitio web del BCP, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturados por los cibercriminales.

3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultado que DIECINUEVE (19) proveedores de seguridad informática, siendo catalogado como **Phishing (suplantación de identidad)**:



- **URL:** hxxps://cmac-ctacna[.]com/view?cgi=v8UfafWduRGMHEGJhtZT
- **Dominio:** cmac-ctacna[.]com
- **Servidor:** Apache
- **IP:** 161[.]97[.]96[.]62
- **Tamaño:** 12.43 KB
- **Texto:** Text/Html
- **SHA-256:** 90451556978d8e7a887a89075bcf990ed62f586d1639e219b535ea8aa325f18c
- **OTRAS DETENCIONES:**

4. Apreciación de la información:

- La presente campaña de Phishing, permite a los actores de amenazas obtener las credenciales de acceso de la banca por internet 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.

5. Recomendaciones:

- No abrir correos ni mensajes de dudosa procedencia.
- Verificar detalladamente las URL de los sitios web.
- Mantener el antivirus actualizado.
- Desconfiar de los enlaces y archivos enviados a través de mensajes o correos electrónicos.
- Prestar atención en los detalles de los mensajes o redes sociales.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta