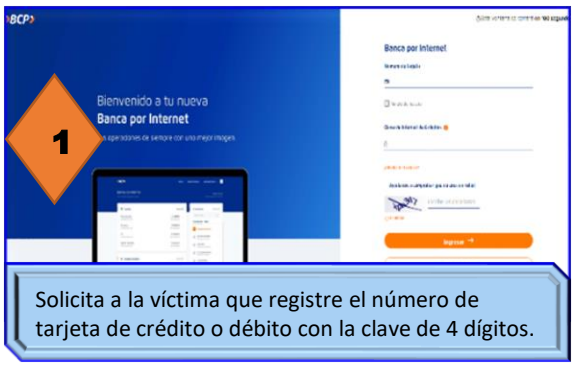
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 005	Fecha: 05-01-2022
		Página: 8 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**			
Nombre de la alerta	Detección de sitio web fraudulento del Banco de 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 subfamilia	G02	
Clasificación temática familia	Fraude			

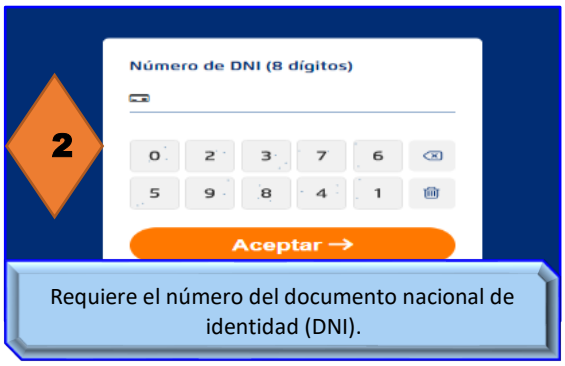
Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que actores de amenazas vienen realizando una campaña de phishing, suplantando el sitio web de la (Banca por internet) del Banco de Crédito del Perú, con la finalidad de obtener información de los usuarios de la entidad financiera como el número de tarjeta de crédito o débito, claves de 4 dígitos, número del Documento Nacional de Identidad, correo electrónico, etc.

2. Detalles del proceso de phishing:



Solicita a la víctima que registre el número de tarjeta de crédito o débito con la clave de 4 dígitos.



Requiere el número del documento nacional de identidad (DNI).

3 Instan a la víctima que registre el número de celular y una vez obtenido los datos de la víctima, redirige al sitio web fraudulento (banca por internet) del Banco de Crédito del Perú. Cabe mencionar que los ciberdelincuentes identifican a la víctima con los apellidos y nombres, a fin de ser más real la web falsa.

3. Comparación del sitio web oficial y fraudulento.

SITIO WEB OFICIAL

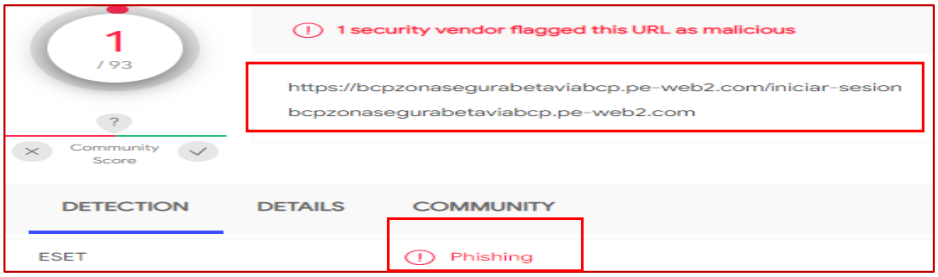
https://bcpzonasegurabeta.viabcp.com/#/iniciar-sesion

SITIO WEB SOSPECHOSA

https://bcpzonasegurabetaviabcp.pe-web2.com/iniciar-sesion

- **Existe una diferencia entre la URL original y la URL fraudulenta.**
- **La URL fraudulenta hxxps://bcpzonasegurabetaviabcp[.]pe-web2[.]com/iniciar-sesion, NO POSEE PROTOCOLO DE SEGURIDAD DE RED (http).**

4. La URL sospechosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo la siguiente información.
   - URL: hxxps://bcpzonasegurabetaviabcp[.]pe-web2[.]com/iniciar-sesion
   - Dominio: pe-web2[.]com
   - Longitud: 14,00 KB
   - SHA-256: 26001b41fd9512f577302cfc7ef4b554c2015b8d9bfacb0a7d2893c9fce8bfec



   - Catalogado como:

5. Comparación de los dominios del sitio web oficial del Banco de Crédito del Perú y la plataforma web sospechosa.

DOMINIO DEL SITIO WEB OFICIAL DEL BANCO DE CRÉDITO DEL PERÚ

```
Domain Name: VIABCP.COM
Registry Domain ID: 25740736_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2020-11-18T23:18:25Z
Creation Date: 2000-04-26T22:48:31Z
Registrar Registration Expiration Date: 2022-04-26T22:48:31Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Reseller:
```

DOMINIO DE LA PLATAFORMA WEB SOSPECHOSA

```
Domain name: pe-web2.com
Registry Domain ID: 2626229679_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2021-07-12T18:25:43.00Z
Registrar Registration Expiration Date: 2022-07-12T18:25:43.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
```

6. Apreciación de la información:
   - La presente campaña de phishing permite a los actores de amenazas obtener información bancaria de los usuarios del Banco del Crédito del Perú. Toda vez que es la entidad financiera más grande y el proveedor líder de servicios financieros integrados en el 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.

7. Recomendaciones:
   - Verificar detalladamente las URL de los sitios web
   - No abrir o descargar archivos sospechosos.
   - No seguir las instrucciones de sitio web sospechoso.
   - Mantener el antivirus actualizado.
   - Comunicar a la entidad financiera si ha realizado un registro de acceso en un sitio web sospechoso.
   - Realizar las actualizaciones correspondientes desde fuentes originales.

Fuentes de información	Análisis propio de redes sociales y fuente abierta