	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°034	Fecha: 08-02-2024
		Página: 13 de 20

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 realizando 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 bancaria de los usuarios de la entidad financiera como números de tarjetas bancarias, clave intranet de seis dígitos, documento de identidad, etc.

2. **DETALLES:**

El proceso del Phishing es el siguiente:

Paso N.º 01

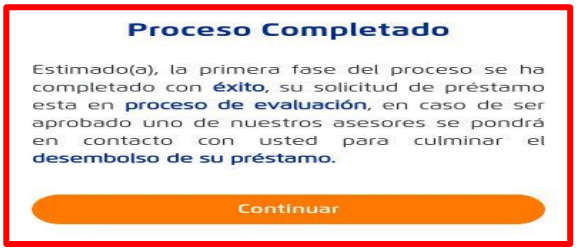
Sitio web fraudulento del banco central del Perú (BCP), solicita a la víctima que registre el monto solicitado del préstamo, cuotas por pagar, Documento Nacional de identidad (DNI) y número de Celular para luego dar clic en <**Empezar**>.

Paso N.º 03

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 caducidad, el código de seguridad (CVV) y la clave de cuatro dígitos utilizado en el cajero automático, para luego dar clic en <**Continuar**>.

Paso N.º 02

Luego de darle clic en <Empezar>, instan a la víctima que registre el número de la tarjeta bancaria y la clave de seis dígitos del intranet, para luego dar clic en <**Continuar**>.



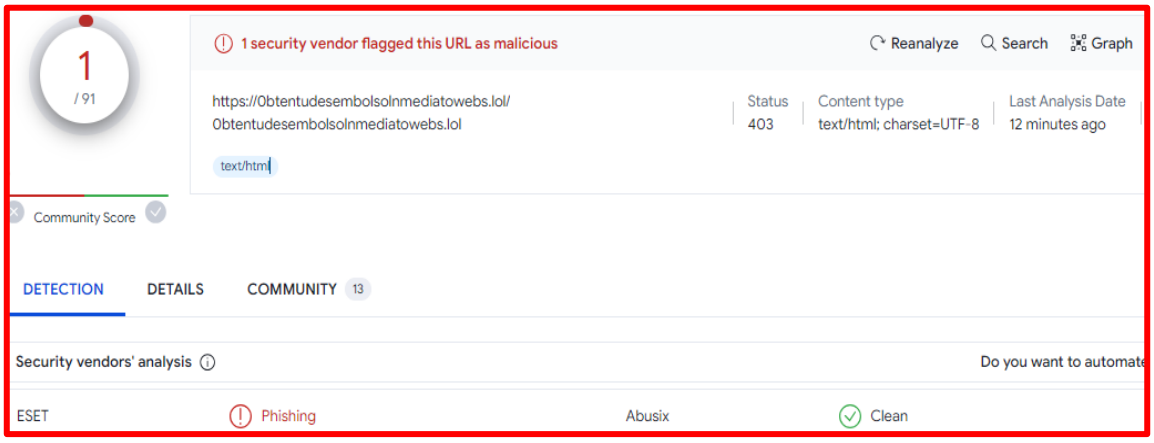
Paso N.º 04

Luego, aparece una pantalla indicando se ha completado con éxito el registro de datos y de ser aprobados el crédito, asesores de la entidad bancaria se pondrán en contacto con la víctima, para luego dar clic en <**Continuar**>. Redirigiendo 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*.

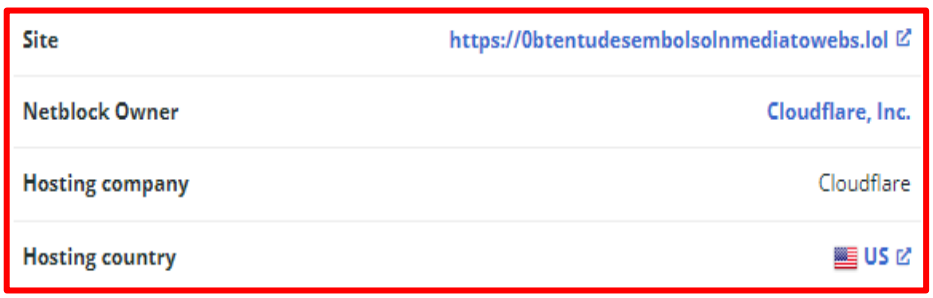
- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL del sitio web fraudulento posee protocolo de seguridad de red (https)
- Existe una similitud entre ambas páginas en imagen, fondo y colores de ambos sitios web.

B. Proveedor de seguridad informática ALERTAN COMO SUPLANTACIÓN DE IDENTIDAD - PHISHING.

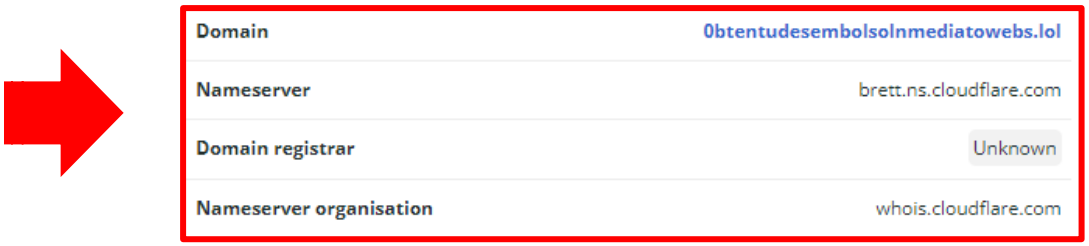


C. Indicadores de compromiso (IoC)

- URL : hXXps://0btentudesembolsolnmediatowebs[.]lol

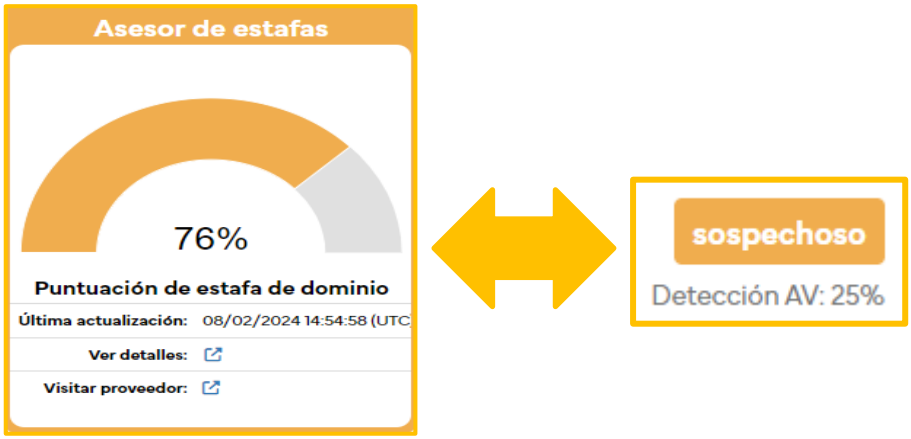


- Dominio : 0btentudesembolsolnmediatowebs[.]lol



- IP : 104[.]21[.]62[.]192

- SHA-256 : afca372f9959cb6c46bde573d25172c1b223dac52cba20ffad3c8fc2ea09cc8e
- Servidor : cloudflare
- Tipo de tex. : Text/Html
- **Otras detenciones**



D. Comparación de Dominios

SITIO WEB OFICIAL

```
Domain Name: VIABCP.COM
Registry Domain ID: 25740736_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2023-12-07T21:04:47Z
Creation Date: 2000-04-26T22:48:31Z
Registrar Registration Expiration Date: 2025-04-
26T22:48:31Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited https://icann.org
/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Banco de Credito del Peru
Registrant Organization: Banco de Credito del Peru
Registrant Street: Calle Centenario 156
Registrant City: Lima
Registrant State/Province: Lima
Registrant Postal Code: Lima12
Registrant Country: PE
Registrant Phone: +51.51120060050692
Registrant Phone Ext:
Registrant Fax: +51.13490492
Registrant Fax Ext:
Registrant Email: dominios@bcp.com.pe
```

SITIO WEB FRAUDULENTA

```
Domain Name: 0BTENTUDESEMBOLSOLNMEDIATOWEBS.LOL
Registry Domain ID: D425643072-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com
Updated Date: 2024-02-08T15:07:43.0Z
Creation Date: 2024-01-17T22:36:22.0Z
Registry Expiry Date: 2025-01-17T23:59:59.0Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Domain Status: serverHold https://icann.org/epp#serverHo
ld
Domain Status: serverTransferProhibited https://icann.or
g/epp#serverTransferProhibited
Domain Status: clientTransferProhibited https://icann.or
g/epp#clientTransferProhibited
Registrant Organization: PrivacyGuardian.org llc
Registrant State/Province: AZ
Registrant Country: US
```

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).

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