	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°058	Fecha: 07-03-2024
		Página: 9 de 12

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:

Paso N.º 01

Sitio web fraudulento del Banco de crédito del Perú (BCP), solicita a la víctima registrar el monto solicitado del préstamo, en cuantas cuotas a pagar, el documento Nacional de identidad (DNI) y el número de Celular. Para luego dar clic en <**Empezar**>.

Paso N.º 02

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

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), la clave de cuatro dígitos utilizado en el cajero automático y el correo electrónico, para luego dar clic en <**Continuar**>.

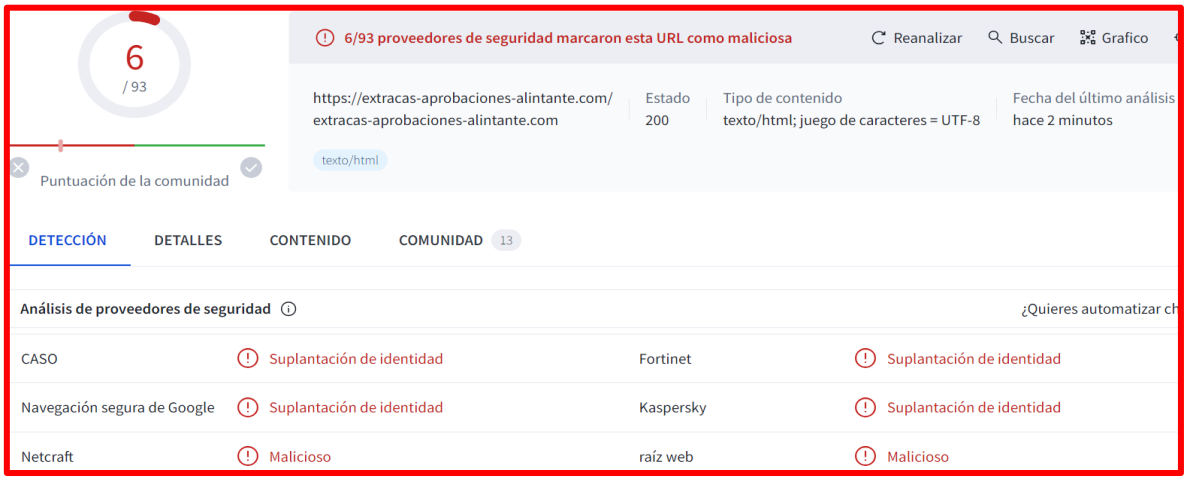
Paso N.º 04

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.*

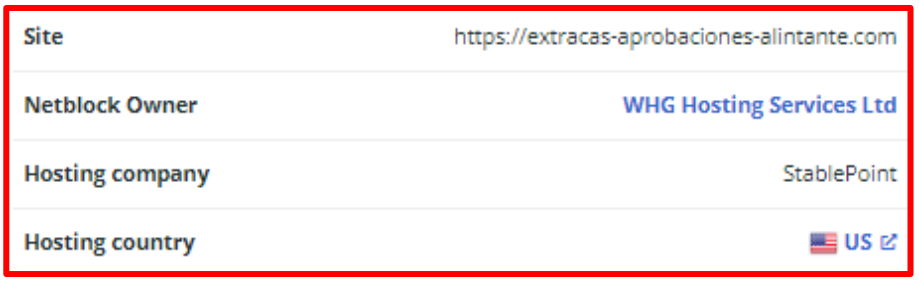
- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL del sitio web fraudulento posee protocolo de seguridad de red (https)
- Existe una similitud entre ambas páginas en imagen, fondo y colores de ambos sitios web.

B. *Hasta la formulación del presente documento, proveedores de seguridad informática HAN ALERTADO COMO SUPLANTACIÓN DE IDENTIDAD - PHISHING.*

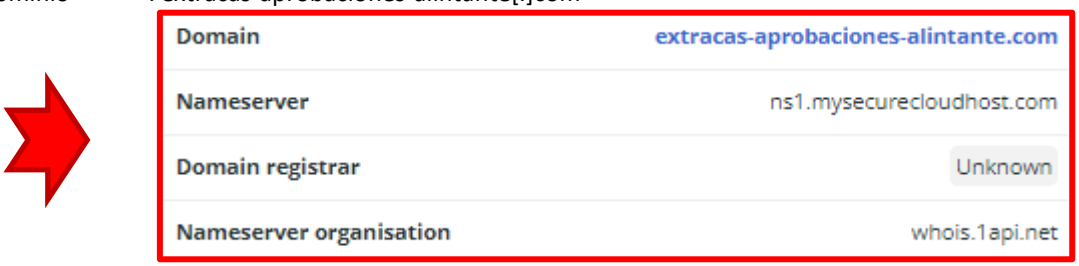


C. *Indicadores de compromiso (IoC)*

- Url : hxxps[:]//extracas-aprobaciones-alintante[.]com



- Dominio : extracas-aprobaciones-alintante[.]com



Domain	extracas-aprobaciones-alintante.com
Nameserver	ns1.mysecurecloudhost.com
Domain registrar	Unknown
Nameserver organisation	whois.1api.net

- IP : 192[.]250[.]239[.]241

IPv4 address (192.250.239.241)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 192.0.0.0-192.255.255.255	United States	NET192	Various Registries (Maintained by ARIN)
↳ 192.250.224.0-192.250.239.255	United States	UK-WHGI-20130606	WHG Hosting Services Ltd
↳ 192.250.239.241	United States	UK-WHGI-20130606	WHG Hosting Services Ltd

- Servidor : LiteSpeed
- SHA-256 : 25ba4abe72dddf18d1b0b793e0f74da7764a9e080d9786c26f5a208441c0b520

D. 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).

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