	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°261	Fecha: 01-11-2023
		Página: 7 de 12

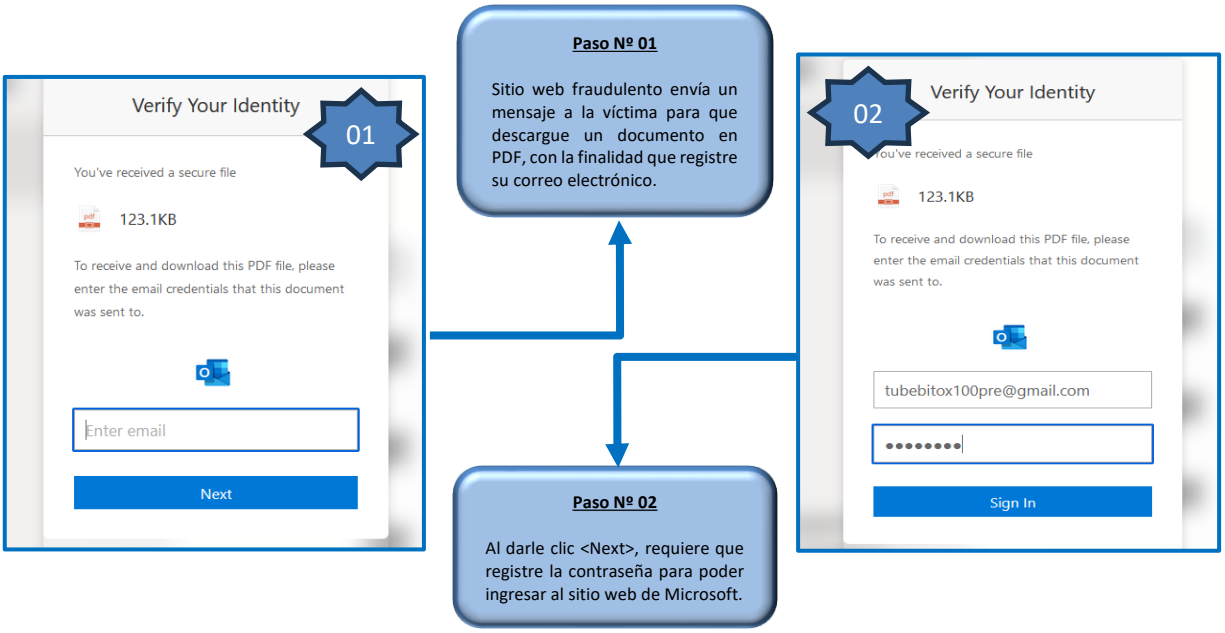
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de Phishing que suplanta la identidad de Outlook		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

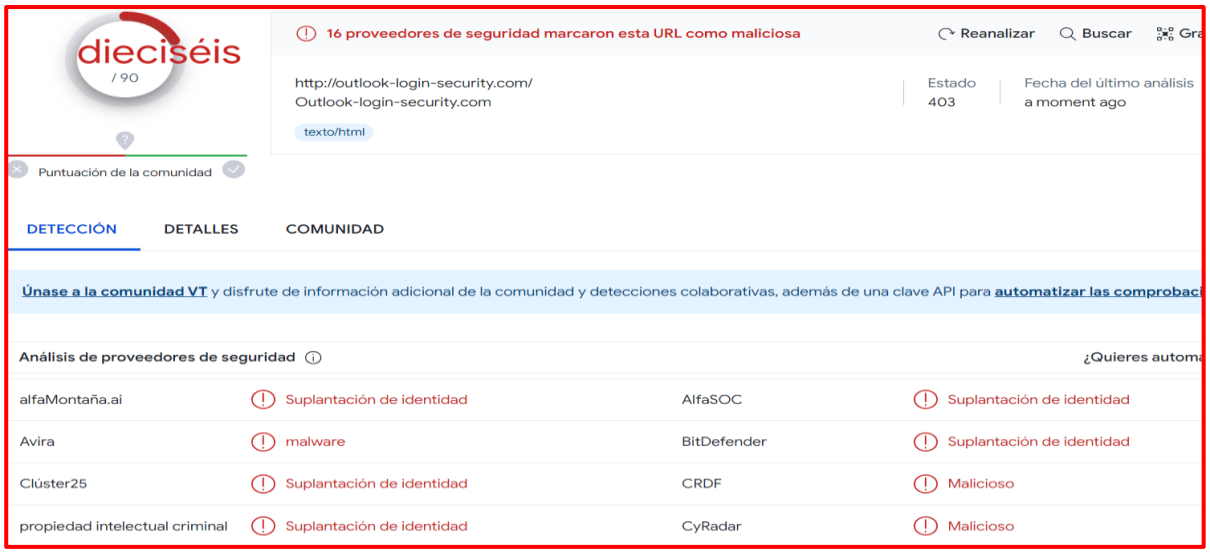
1. **ANTECEDENTES:**

   A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes se encuentran desarrollando una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad del sitio oficial de "Outlook"; con el objetivo de acceder u obtener credenciales de inicio de sesión de las posibles víctimas.

2. **DETALLES:**

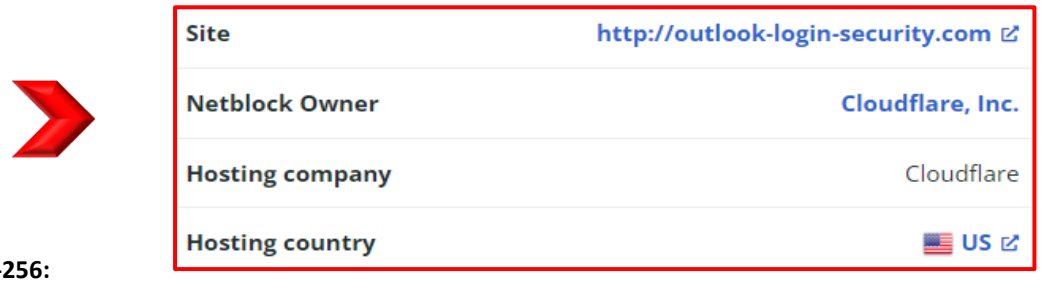


A. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**



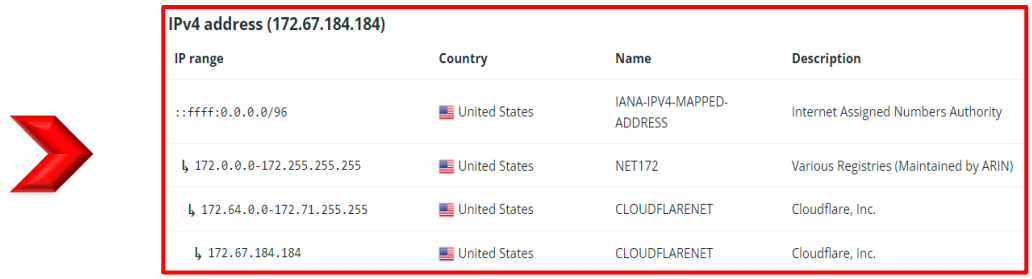
Indicadores de compromiso:

I. URL: hxxp://outlook-login-security[.]com/



II. SHA-256:
2afbc0512e96a9eb7b49063af03d8b441eb2a6d67dc71d9cb2f96617150b15e9

III. IP: 172[.]67[.]184[.]184



IV. DOMINIO: outlook-login-security[.]com

Domain	outlook-login-security.com
Nameserver	frank.ns.cloudflare.com
Domain registrar	Unknown
Nameserver organisation	whois.cloudflare.com

B. Otras detecciones:

C. Cómo funciona el Phishing:

- Los correos electrónicos incluyen enlaces a sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
- Medios de propagación del Phishing: WhatsApp, Telegram, redes sociales, SMS entre otros.
- Los ciberdelincuentes intentan suplantar a una entidad legitima (organismo público o privado, entidad financiera, servicio técnico, etc.)

D. Referencia:

- Phishing o suplantación de identidad: Es un método que los ciberdelincuentes, utilizan para engañar a los usuarios para conseguir que revele información personal, como contraseñas, datos de tarjetas de créditos, números de cuentas bancarias, entre otros.

3. RECOMENDACIONES:

- Evitar acceder a enlaces que llegan inesperadamente por correo electrónico u otros medios.
- No proporcionar datos personales (contraseñas, tarjetas, cuentas bancarias, etc.) por correo, teléfono o SMS.
- No introducir datos confidenciales en sitios web sospechosas o de dudosa procedencia.
- Verificar la fuente de información de tus correos entrantes.
- Introducir tus datos únicamente en webs seguras.
- Tener siempre actualizado el sistema operativo y el antivirus. En el caso del antivirus, comprobar que está activo.

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

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°261	Fecha: 31-10-2023
		Página: 10 de 12

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Campaña de Phishing que suplanta 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 Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. **ANTECEDENTES:**

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo ataques avanzados de Phishing, dirigidos a usuarios de la identidad del Banco de Crédito del Perú (BCP), con el objetivo robar credenciales de acceso, datos personales y bancarios.

2. **DETALLES:**

Detalles del proceso de estafa.

Imagen 1:

Para solicitar un préstamo el atacante le solicita a la víctima registrar el número del Documento Nacional de Identidad (DNI), el monto del préstamo solicitado y el número de Celular.

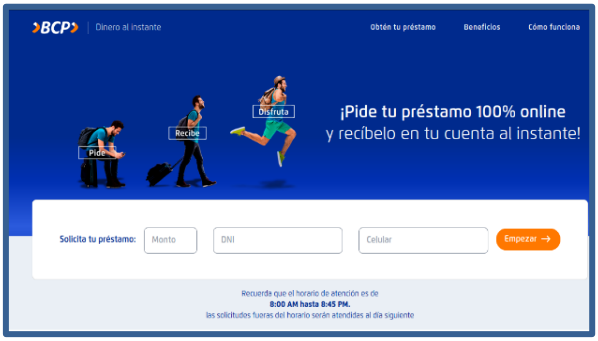


Imagen 2:

Luego de completar con lo requerido, le solicita a la víctima el número de tarjeta de crédito o débito y clave de seis dígitos (INTRANET), para luego dar clic en <Continuar>.

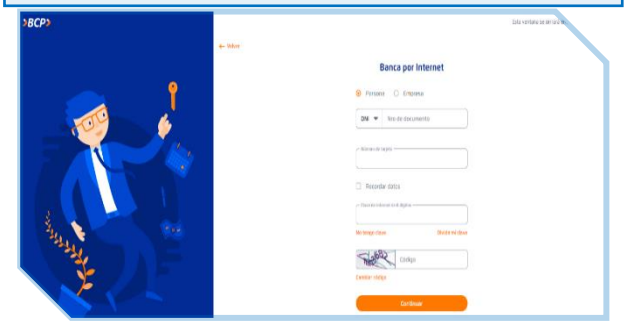
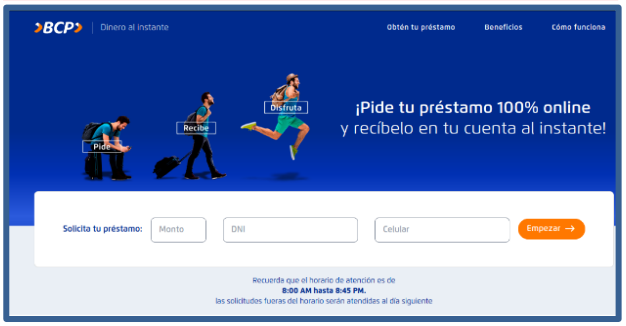
Imagen 3:

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

Imagen 4:

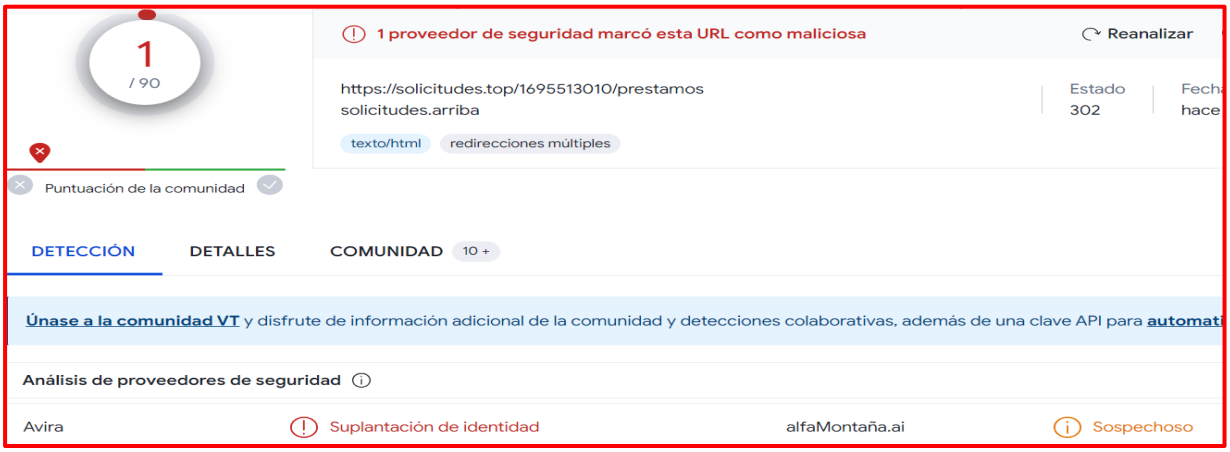
Luego, aparece una pantalla indicando que el proceso se ha completado con éxito y que un asesor de la entidad se comunicará con la víctima, para culminar con el desembolso del préstamo, para luego hacer clic en <Continuar>.

A. Comparación del sitio web oficial y sitio web falso del BCP:

SITIO WEB OFICIAL hxxps://loginunico.viabcp.com/#/tarjeta-sesion	SITIO WEB FRAUDULENTO hxxps://solicitudes[.]top/1695513010/prestamos
	

- No existe una similitud entre el fondo y forma de cada sitio web.
- Hay diferencia en el dominio, debido a que el sitio web fraudulento no coincide con el sitio oficial del BCP.
- La URL posee el ***PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS),*** esto hace que la víctima registre sus datos personales en dichos sitio web.

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



C. Indicadores de compromiso (IoC)

- Dominio : solicitudes[.]top
- SHA-256 : 0bad283f8b8cf8313b26a6ca57a87fe2366a77fee12e4725da298ad67cdcb4f3
- IP : 172[.]67[.]170[.]148
- Servidor : cloudflare
- Tipo : Text/Html

3. RECOMENDACIONES:

- Verificar detalladamente la URL, que corresponda al sitio web oficial.
- Tener en cuenta que las entidades bancarias no solicitan actualización de datos confidenciales de manera online.
- Ingresar sólo desde fuentes oficiales.
- No seguir las instrucciones de algún sitio web sospechoso.
- Mantener el antivirus actualizado.
- Evitar compartir la URL con amigos y/o familiares.

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