	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°224	Fecha: 22-09-2023
		Página: 9 de 11

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de Phishing suplantando al BBVA		
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 una campaña de Phishing, dirigidas a usuarios de la entidad bancaria BBVA, con el objetivo robar las credenciales de acceso al servicio de banca en línea.

2. **DETALLES:**

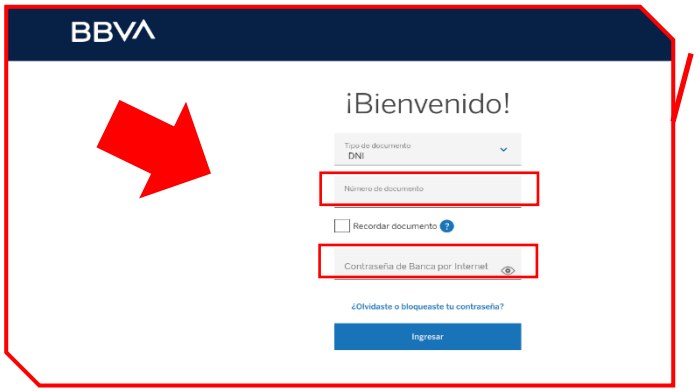


Imagen 1. Página web falsa, solicita al usuario que ingrese las credenciales de acceso a la cuenta en línea.

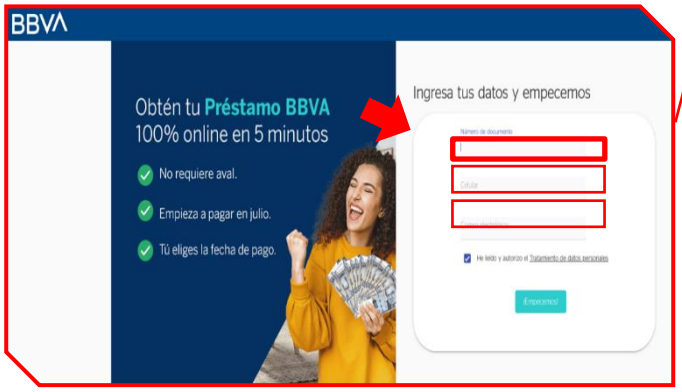
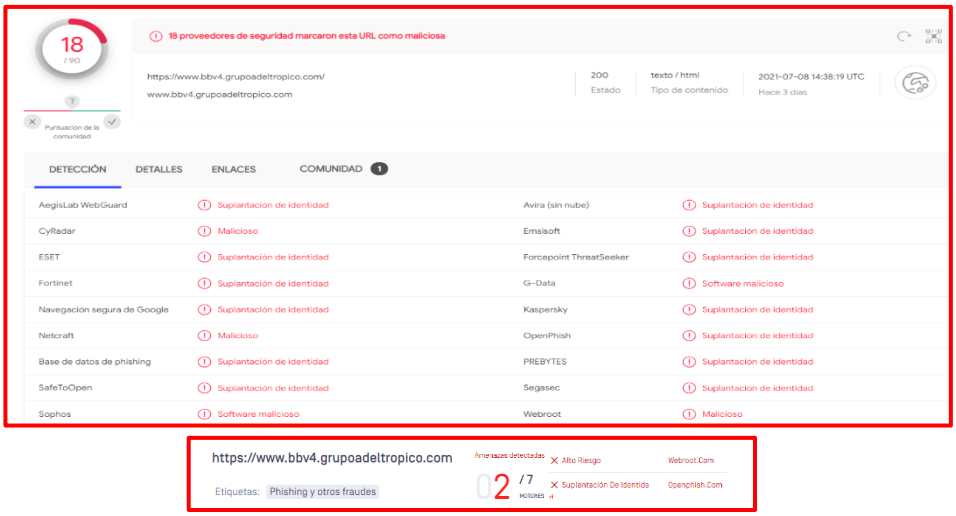


Imagen 2. Solicita al usuario que ingrese sus datos personales (Número de DNI, teléfono y correo electrónico).

Imagen 3. Una vez que el Phishing ha logrado capturar los datos de la víctima, aparece en la pantalla el siguiente mensaje: ***"¡Felicidades tienes un préstamo con Garantía aprobado!".*** Concretándose la estafa.

A. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo la siguiente información:

- URL Malicioso: hXXps[:]//www[.]bbv4[.]grupoadeltropico[.]com/
- Dominio: www[.}bbv4[.]grupoadeltropico[.]com
- Código: 200
- Longitud: 117,89 KB
- SHA-256: ab279ab509b7ff0a38bf4f3b7e54e822a09f049a59c24f9996194ab28f4dbd89



- Lista negra | IP: 162[.]241[.]60[.]213

B. 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.)

C. 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:

- No abrir correos de usuarios desconocidos o que no hayas solicitado, elimínalos directamente.
- Cerrar todas las aplicaciones antes de acceder a la web del banco.
- Teclear directamente la dirección URL en la barra de direcciones al momento de visitar el sitio web del banco.
- Tener precaución al seguir enlaces y descargar ficheros adjuntos de correos, aunque sean de contactos conocidos.
- Acudir a una sucursal o comunicarse con la institución financiera.
- No olvidar siempre estar alerta, aunque parezcan buenas noticias.

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