	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°231	Fecha: 01-10-2023
		Página: 6 de 11

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de Phishing que suplanta la entidad bancaria de 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 avanzados ataques cibernéticos, por medio de envíos de correos electrónicos fraudulentos, o también conocidos como Phishing, simulado ser la entidad bancaria BBVA, en cual tiene el objetivo de robar credenciales de acceso, datos personales y bancarios, de las potenciales víctimas.

2. **DETALLES:**

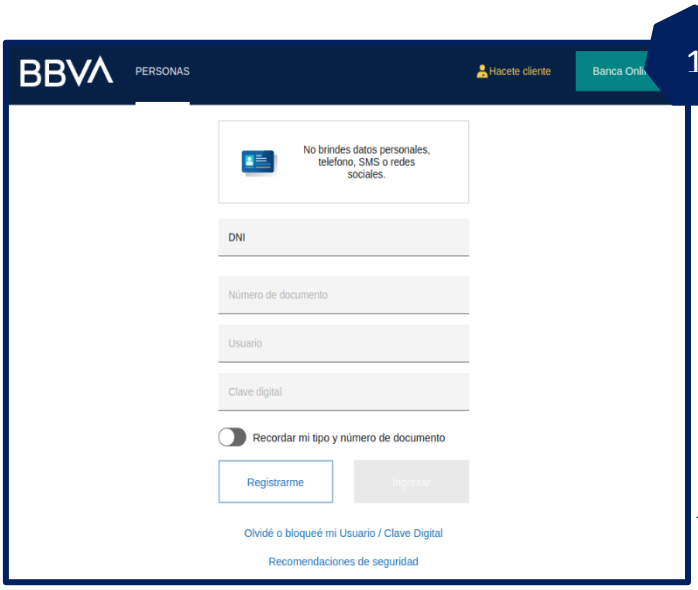


Imagen 1.
Plataforma web fraudulenta del Banco BBVA, solicita a la victima el documento de identidad (DNI), el usuario y clave digital.

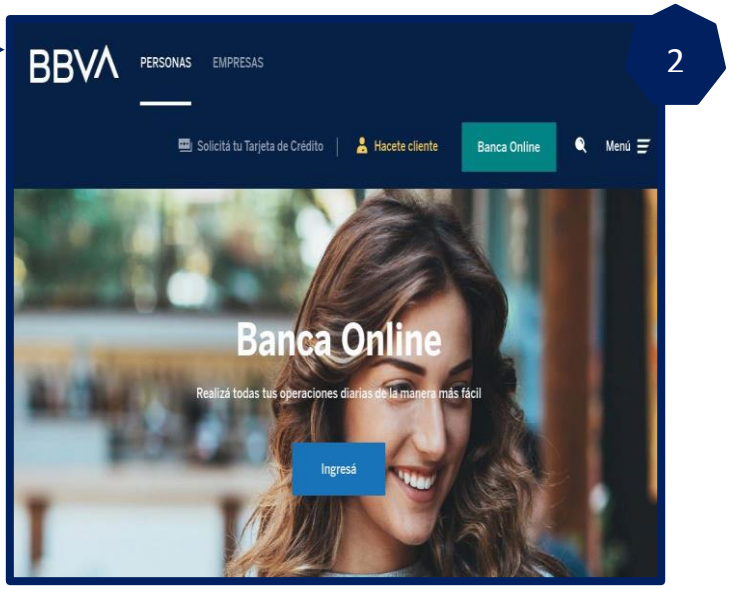
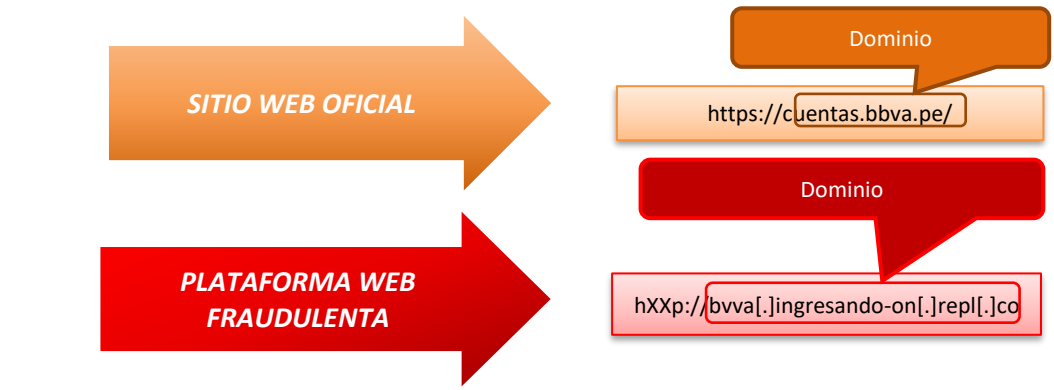


Imagen 2.
Después de completar lo requerido por los atacantes, dentro de unos segundos es redirigido, a la web oficial del banco BBVA, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturados por los cibercriminales.

A) Comparación del sitio web oficial y sitio web fraudulento del banco BBVA:



- Existe diferencia en el dominio de sitio web fraudulento, no coincide con el oficial.
- El sitio web fraudulento no posee el **PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS).**

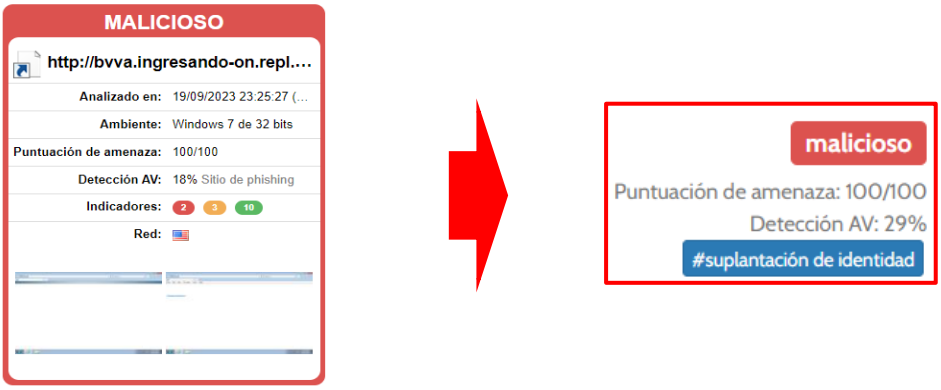
B) Proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD – PHISHING**

ADMINUSLabs	Malicioso	AlphaSOC	Suplantación de identidad
Avira	Suplantación de identidad	BitDefender	Malware
CRDF	Malicioso	CyRadar	Malicioso
G-datos	Malware	kaspersky	Suplantación de identidad
Leonico	Malicioso	Búsqueda segura	Malicioso
VIPRE	Malicioso	raíz web	Malicioso

C) Indicadores de compromiso:

- URL: hxxp[:]//bvva[.]ingresando-on[.]repl[.]co/
- Dominio: bvva[.]ingresando-on[.]repl[.]co
- IP: 35[.]186[.]245[.]55
- SHA-256: 69dfff6256d33c9200093df3c87ae7988e28deede85222038316591d47dda9db

D) Otros resultados del análisis:



3. RECOMENDACIONES:

- Verificar detalladamente la URL, que corresponda al sitio web oficial del banco BBVA.
- Evitar seguir las instrucciones de sitio web sospechoso o de dudosa procedencia.
- Mantener el antivirus actualizado, ya que es la primera barrera ante posibles ataques cibernéticos.
- Evitar compartir la URL con amigos y/o familiares.
- Ingresar desde fuentes oficiales (www.bbva.pe).

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