	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 103	Fecha: 03-05-2023
		Página 10 de 13

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 subfamilia	G02
Clasificación temática familia	Fraude		

Descripción

1. 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, simulando ser la entidad bancaria BBVA, en el cual tiene el objetivo de robar credenciales de acceso, datos personales y/o bancarios.

2. Detalles del proceso de Phishing:

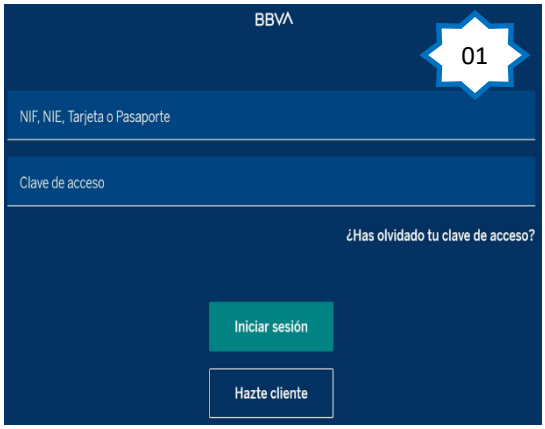

Imagen 1.

Sitio web fraudulenta del Banco BBVA, solicita a la víctima el documento de identidad (NIF, NIE, TARJETA O PASAPORTE) y clave digital para ingresar.

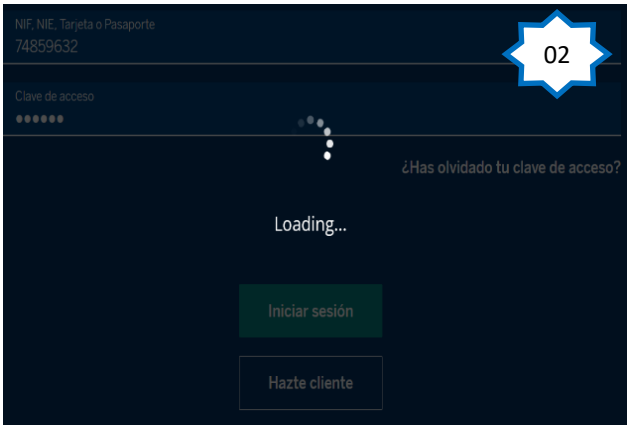

Imagen 2.

Después de completar lo requerido por los atacantes, dentro de unos segundos sale una ventana emergente de espera, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturados por los cibercriminales.

SITIO WEB OFICIAL

Dominio

https://www.bbva.pe/

PLATAFORMA WEB FRAUDULENTA

Dominio

hxxp://bbva-seguridadaprobar[.]com/login[.]php

- No existe una similitud entre el fondo y forma de cada sitio web (oficial y fraudulento).
- El sitio web fraudulento no poseen el ***PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS)***.

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

- Indicadores de compromiso:
  - **URL**: hxxp://bbva-seguridadaprobar[.]com/login[.]php
  - **Dominio**: bbva-seguridadaprobar[.]com
  - **SHA-256**: 52445023c6c103d5d2f5f855d099445e785f5794143f0ef636cffd5233c75df9
  - **IP**: 185[.]156[.]72[.]17
  - **SERVIDOR:** LiteSpeed
  - **TIPO:** texto/html
  - **Otros resultados del análisis**:

4. Apreciación de la información:

- La presente campaña de Phishing, permite a los actores de amenazas obtener las credenciales de acceso a la banca por internet de los usuarios del Banco BBVA.

- 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.

5. Que es un Phishing:

- Es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.