	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 135	Fecha: 09-06-2023
		Página 8 de 11

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de suplantación de 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 cual tiene el objetivo de robar credenciales de acceso, datos personales y/o bancarios.

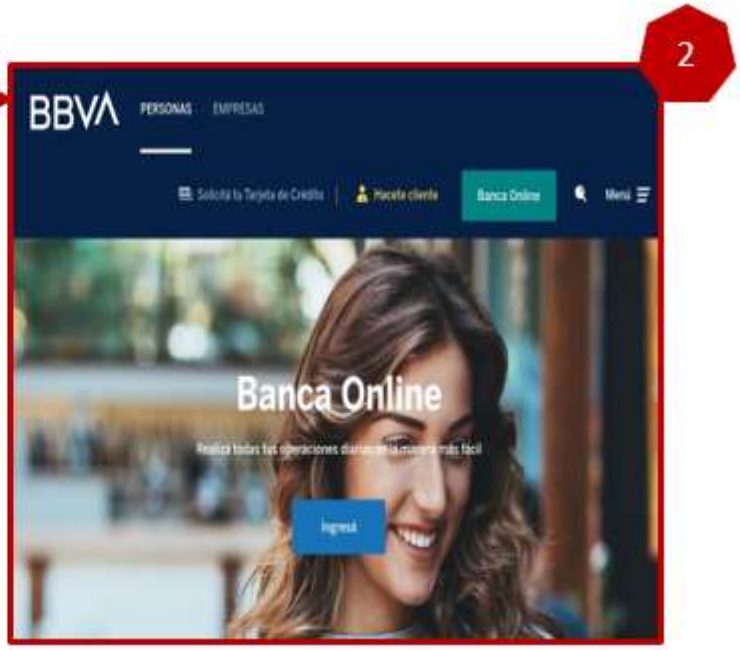
2. Detalles del proceso de Phishing:

Imagen 1.

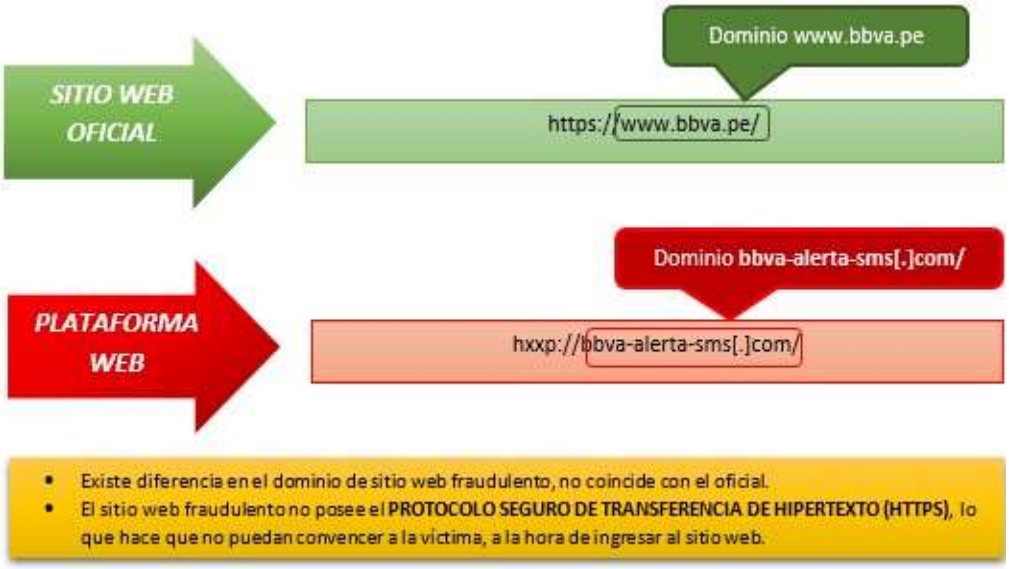
Plataforma web fraudulenta del Banco BBVA, solicita a la victima el documento de identidad (DNI), el usuario y clave digital.

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.



3. Comparación del sitio web oficial y sitio web fraudulento del banco BBVA:

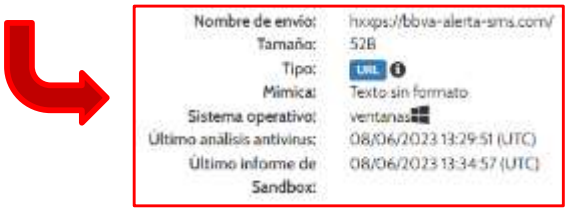


4. Proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD – PHISHING**

alphaMountain.ai	Suplantación de identidad	Avira	Suplantación de identidad
BitDefender	Suplantación de identidad	CRDF	Malicioso
CyRadar	Malicioso	ESET	Suplantación de identidad
Fortinet	Suplantación de identidad	G-datos	Suplantación de identidad
Navegación segura de Google	Suplantación de identidad	Seguridad Heimdal	Suplantación de identidad
Leonico	Suplantación de identidad	Búsqueda segura	Malicioso
Sophos	Suplantación de identidad	Inteligencia de amenazas de Viettel	Suplantación de identidad
VIPRE	Malicioso	raíz web	Malicioso
Buscador de amenazas de Forcepoint	Sospechoso	Abusix	Limpio

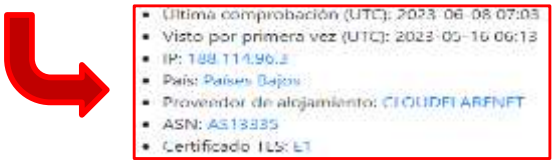
5. Indicadores de compromiso:

a) URL: hxxp:// bbva-alerta-sms[.]com

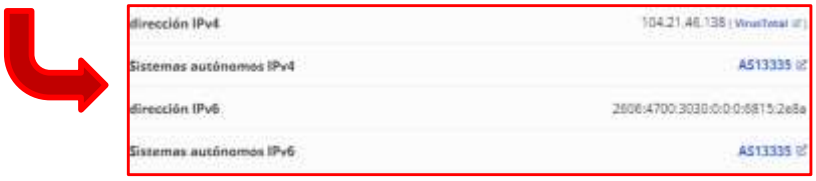


b) Dominio: bbva-alerta-sms[.]com

c) Proveedor de alojamiento: Cloudflarenet



d) IP: 188[.]114[.]96[.]3



e) SHA – 256: c44b3da1c3752dc73d73f6bf37d871884181d809ab1d921792dc5a52a1aca579

6. Otros resultados del análisis:

7. Cómo funciona el Phishing:

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

8. Referencia:

a) 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.

9. Recomendaciones:

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

Fuentes de información	Análisis propio de redes sociales y fuente abierta