	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°291	Fecha: 06-12-2023
		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 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/o bancarios.

2. DETALLES:

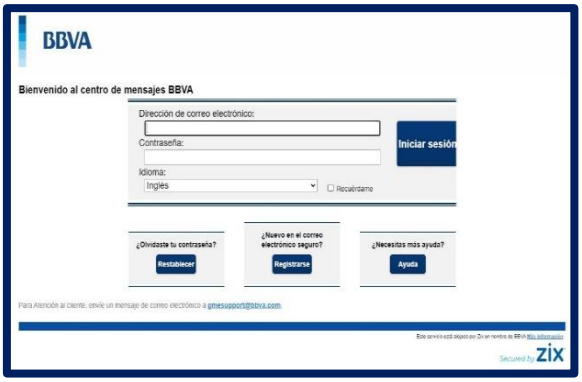


IMAGEN 1:

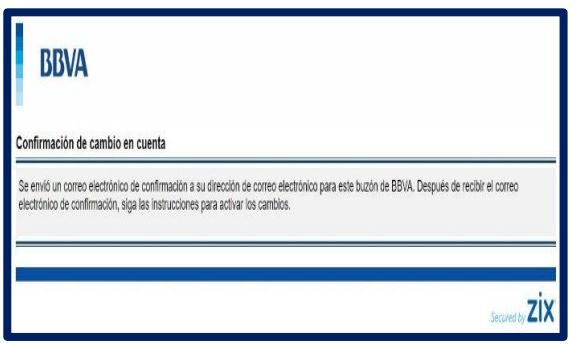
Sitio web fraudulenta del Banco BBVA, solicita a las víctimas registrar la dirección del correo electrónico, la contraseña y el idioma para iniciar sesión.

IMAGEN 2:

Luego de no poder iniciar sesión y darle click en "olvidaste la contraseña" requiere registrar la dirección del correo electrónico, el tipo de idioma y volver a introducir la contraseña para continuar

IMAGEN 3:

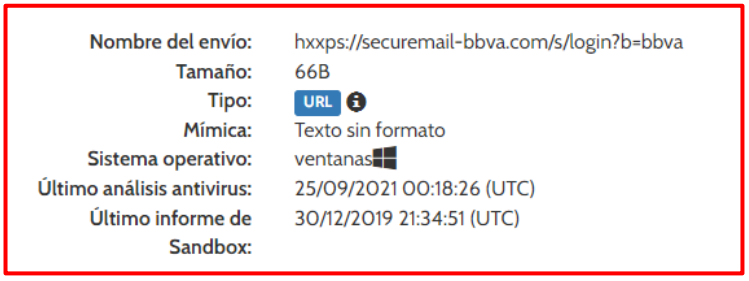
Por último, solicita a la víctima confirmar la cuenta, lo cual tendría que ingresar al correo electrónico y completar lo requerido por los atacantes, para luego informar a la víctima que ha ocurrido un error de autenticación; sin embargo, los datos fueron capturados por los cibercriminales.



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

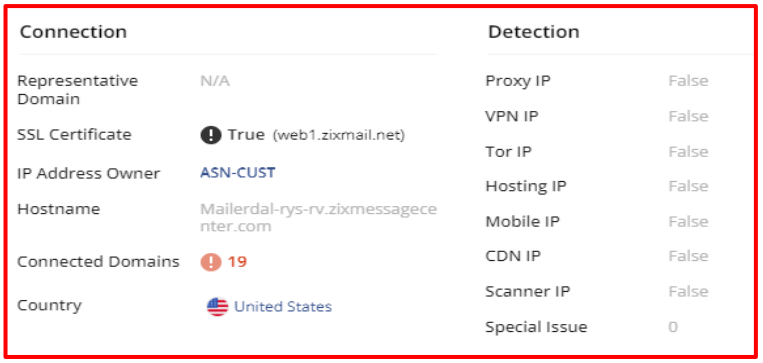
a) Indicadores de compromisos:

I. URL: hxxps[:]//securemail-bbva[.]com/s/login?b=bbva

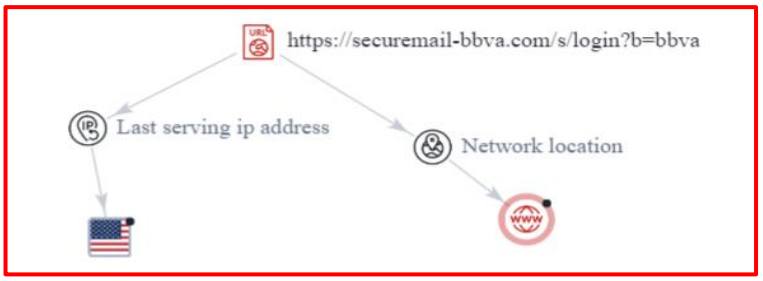


II. SHA-256: bc2db9b94118ed9f2abaeb0b429905fcd15c91fd1372c9d4a1e3987338a40f3d

III. IP: 207[.]195[.]182[.]15



IV. Tipología:



Se puede aprecia como la URL, esta alojada en un servidor ubicado en EE. UU.

B. Se hallaron **06 proveedores** de seguridad que marcaron este dominio como malicioso.

Avira	Phishing	CRDF	Malicious
G-Data	Phishing	OpenPhish	Phishing
Seclookup	Malicious	VIPRE	Malicious

C. Otras detecciones:

D. Apreciación de la información:

- Es una técnica de ingeniería social basada en el engaño, que usan los ciberdelincuentes, con la finalidad de obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de las credenciales de acceso a los diferentes sitios web e información sensible.

E. 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.

F. 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.