	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°268		Fecha: 09-11-2023
			Página: 11 de 14
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:

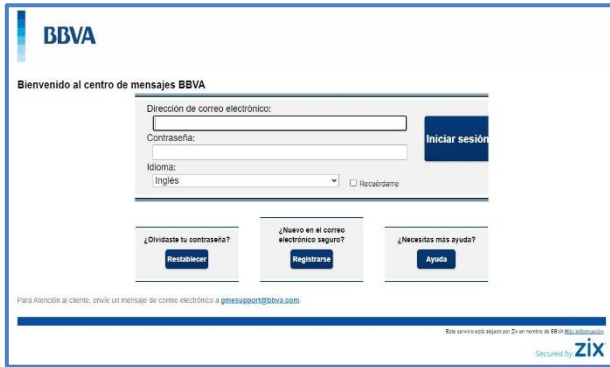


Imagen 1.
Sitio web fraudulenta del Banco BBVA, solicita a las víctimas registrar la dirección del correo electrónico, la contraseña y el idioma para iniciar sesión.

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.

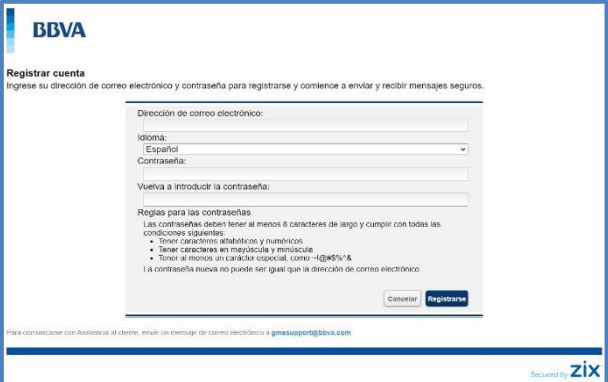
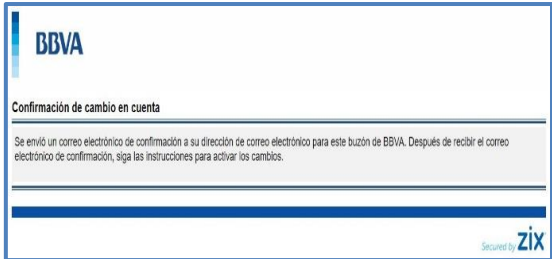
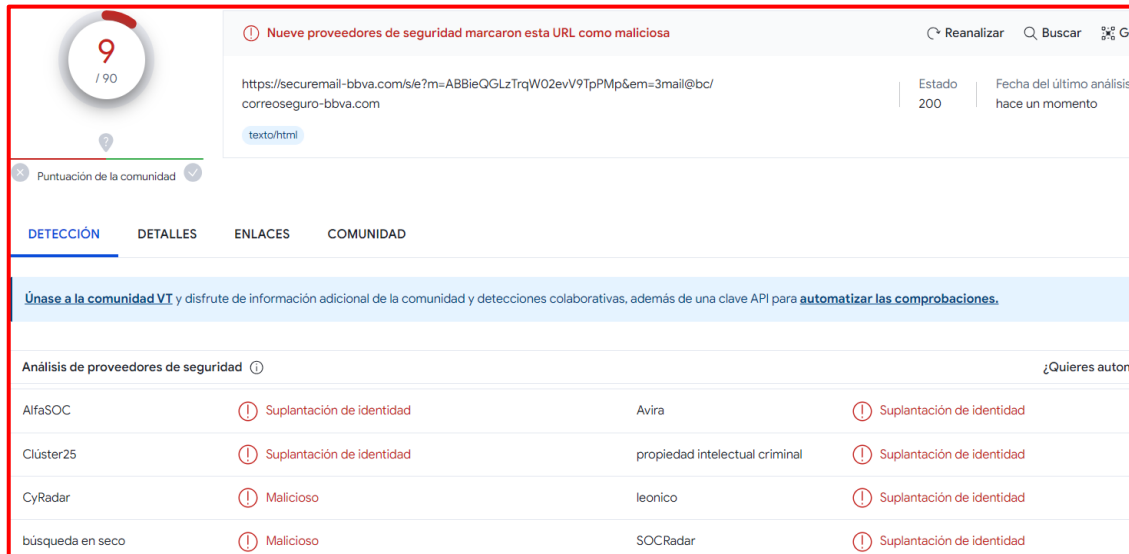


Imagen 3.
Por último, solicita a la víctima confirmar la cuenta, lo cual tendría que ingresar al correo electrónico y completar lo requerido por los atacantes, para luego informar a la víctima que ha ocurrido un error de autenticación; sin embargo, los datos fueron capturados por los cibercriminales.



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



Nueve proveedores de seguridad marcaron esta URL como maliciosa

<https://securemail-bbva.com/s/e?m=ABBiEQLzTrqW02evV9TpPMp&em=3mail@b/c/correoseguro-bbva.com>

Estado: 200 | Fecha del último análisis: hace un momento

Puntuación de la comunidad: 9 / 90

DETECCIÓN | DETALLES | ENLACES | COMUNIDAD

Únase a la comunidad VT y disfrute de información adicional de la comunidad y detecciones colaborativas, además de una clave API para automatizar las comprobaciones.

Análisis de proveedores de seguridad

Proveedor	Alerta	Detalles	Proveedor	Alerta
AlfaSOC	Suplantación de identidad		Avira	Suplantación de identidad
Clúster25	Suplantación de identidad		propiedad intelectual criminal	Suplantación de identidad
CyRadar	Malicioso		leonico	Suplantación de identidad
búsqueda en seco	Malicioso		SOCRadar	Suplantación de identidad

Indicadores de compromiso:

- **URL:** `hxxps://securemail-bbva[.]com/s/e?m=ABBiEQLzTrqW02evV9TpPMp&em=3mail@b[.]c/`



Site	https://securemail-bbva.com
Netblock Owner	Com2.com Inc.
Hosting company	Erado Message Control Solutions
Hosting country	US

- **Dominio:** `securemail-bbva[.]com`



Domain	securemail-bbva.com
Nameserver	a1-166.akam.net
Domain registrar	tu cows.com
Nameserver organisation	whois.markmonitor.com


- **IP:** `207[.]195[.]182[.]15`



IP range	Country	Name	Description
::ffff:0:0:0:0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
207.0.0-207.255.255	United States	NET207	American Registry for Internet Numbers
207.195.160.0-207.195.191.255	United States	CM2-A-BLK-1	Com2.com Inc.
207.195.182.15	United States	CM2-A-BLK-1	Com2.com Inc.

- **Server:** Apache
- **SHA-256:** `cca705a84a83d7a858b8435aff11da900e3a6c133c21f5efe9dfa723338d477d`
- **Tipo de Contexto:** Text/Html

○ **Otros resultados del análisis:**

SOSPECHOSO	SOSPECHOSO
	



malicioso

Puntuación de amenaza: 100/100

Detección AV: 30%

#suplantación de identidad

B. 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 envíos 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.

C. 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.

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.
------------------------	---