	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°165	**Fecha: 13-07-2023**
		Página: 9 de 12

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de Alerta	Nueva campaña de Phishing que suplanta la entidad bancaria de BBVA		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medio de Propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Subfamilia	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.

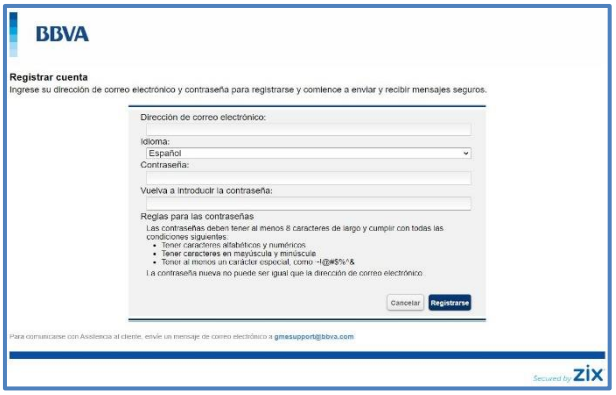
2. **DETALLES**:

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.



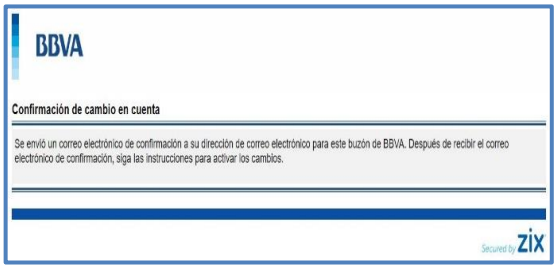
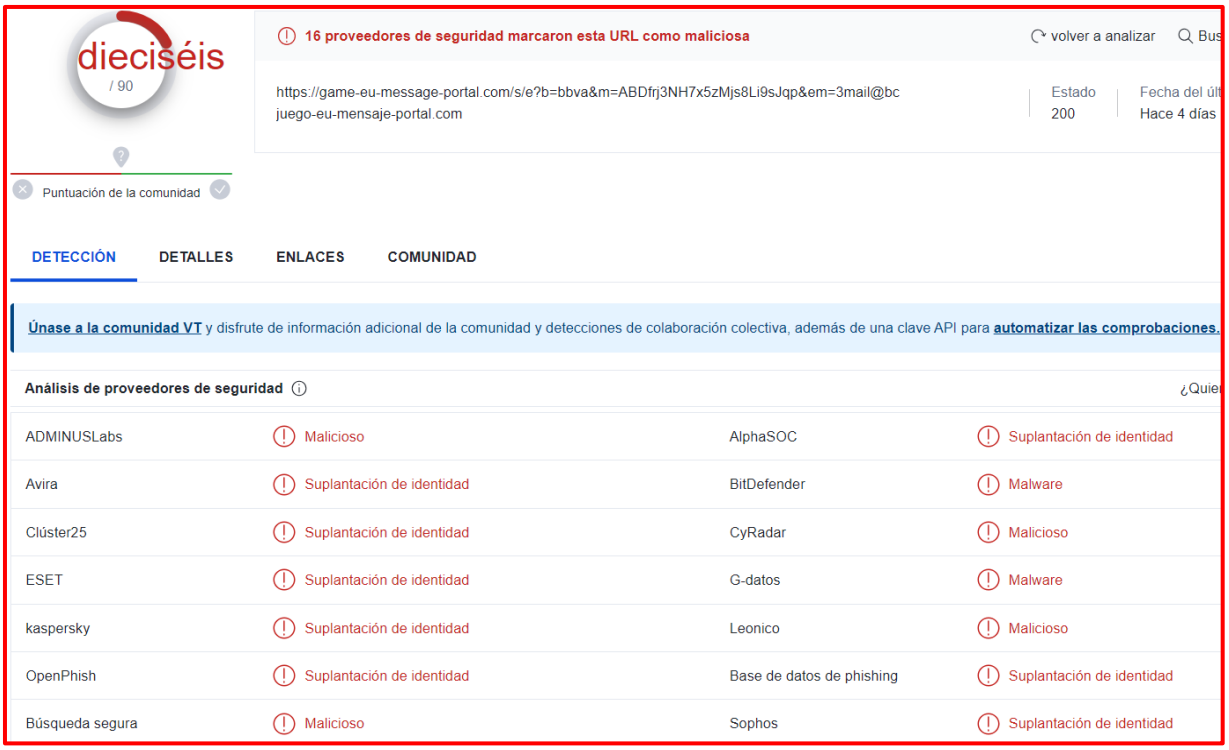


Imagen 3.

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**:



dieciséis / 90

Puntuación de la comunidad

16 proveedores de seguridad marcaron esta URL como maliciosa

volver a analizar | Bus

https://game-eu-message-portal.com/s/e?b=bbva&m=ABDfrj3NH7x5zMjs8Li9sJqp&em=3mail@bc
juego-eu-mensaje-portal.com

Estado: 200 | Fecha del últ: Hace 4 días

DETECCIÓN | DETALLES | ENLACES | COMUNIDAD

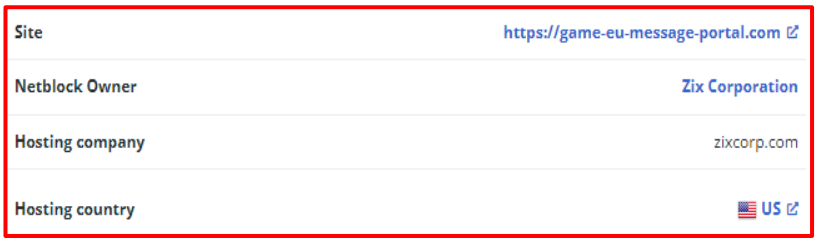
Únase a la comunidad VT y disfrute de información adicional de la comunidad y detecciones de colaboración colectiva, además de una clave API para automatizar las comprobaciones.

Análisis de proveedores de seguridad ¿Quie

ADMINUSLabs	Malicioso	AlphaSOC	Suplantación de identidad
Avira	Suplantación de identidad	BitDefender	Malware
Clúster25	Suplantación de identidad	CyRadar	Malicioso
ESET	Suplantación de identidad	G-datos	Malware
kaspersky	Suplantación de identidad	Leonico	Malicioso
OpenPhish	Suplantación de identidad	Base de datos de phishing	Suplantación de identidad
Búsqueda segura	Malicioso	Sophos	Suplantación de identidad

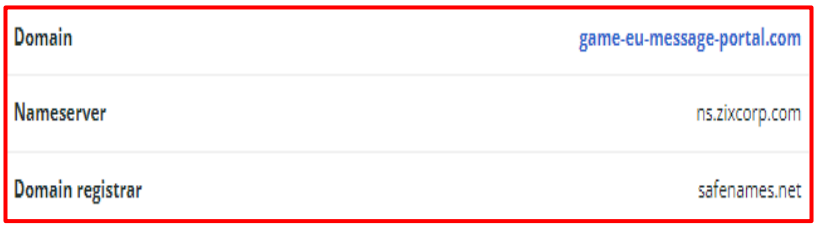
B. Indicadores de compromiso:

- **URL**: hxxps://game-eu-message-portal.com/s/e?b=bbva&m=ABDfrj3NH7x5zMjs8Li9sJqp&em=3mail%40b.c



Site	https://game-eu-message-portal.com
Netblock Owner	Zix Corporation
Hosting company	zixcorp.com
Hosting country	US

- **Dominio**: game-eu-message-portal.com



Domain	game-eu-message-portal.com
Nameserver	ns.zixcorp.com
Domain registrar	safenames.net

- **IP**: 91[.]209[.]6[.]51

IPv4 address (91.209.6.51)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 91.0.0.0-91.255.255.255	Netherlands	91-RIPE	RIPE Network Coordination Centre
↳ 91.209.6.0-91.209.6.255	United States	Zixcorp	Zix Corporation
↳ 91.209.6.51	United States	Zixcorp	Zix Corporation

- **Server:** Apache
- **SHA-256**: eee3a377451ac15aff7cfe59d614172193ad49437072ed7286c66aeda3787c30
- **Tipo de Contexto:** Text/Html

- **Otros resultados del analisis**:

C. 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.

D. 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