	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°167	**Fecha: 16-07-2023** **Página: 6 de 12**

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**			
Nombre de Alerta	Suplantación de la identidad web de la Red Social Facebook			
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 se encuentran desarrollando una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad de la Red Social Facebook, con el objetivo de acceder u obtener credenciales de inicio de sesión de las posibles víctimas.

2. DETALLES:

Proceso de Phishing.

Sitio web fraudulento; donde los ciberdelincuentes buscan persuadir a sus víctimas, solicitando ingresar sus credenciales de acceso.

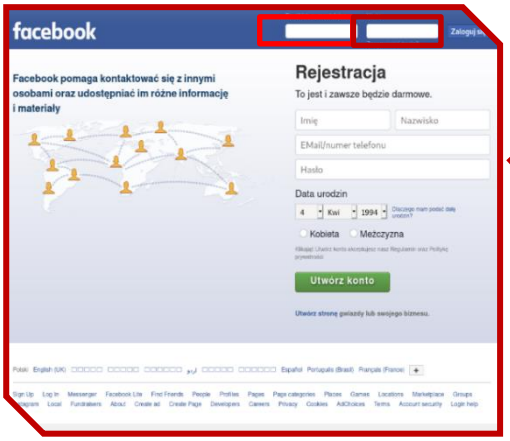


Figura 1. El sitio fraudulento que suplanta la identidad de Facebook, solicita al usuario que ingrese de las credenciales de acceso de inicio de sesión (correo electrónico o número de celular y la clave o contraseña).

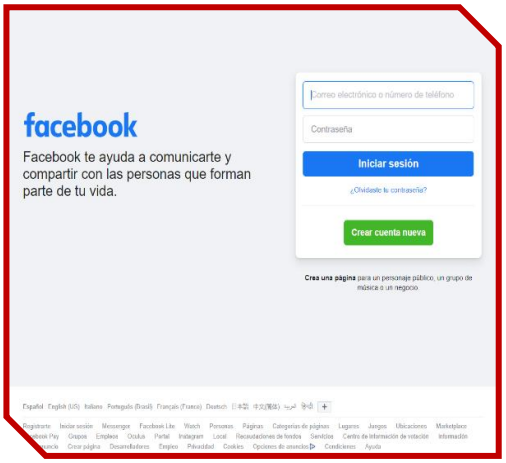
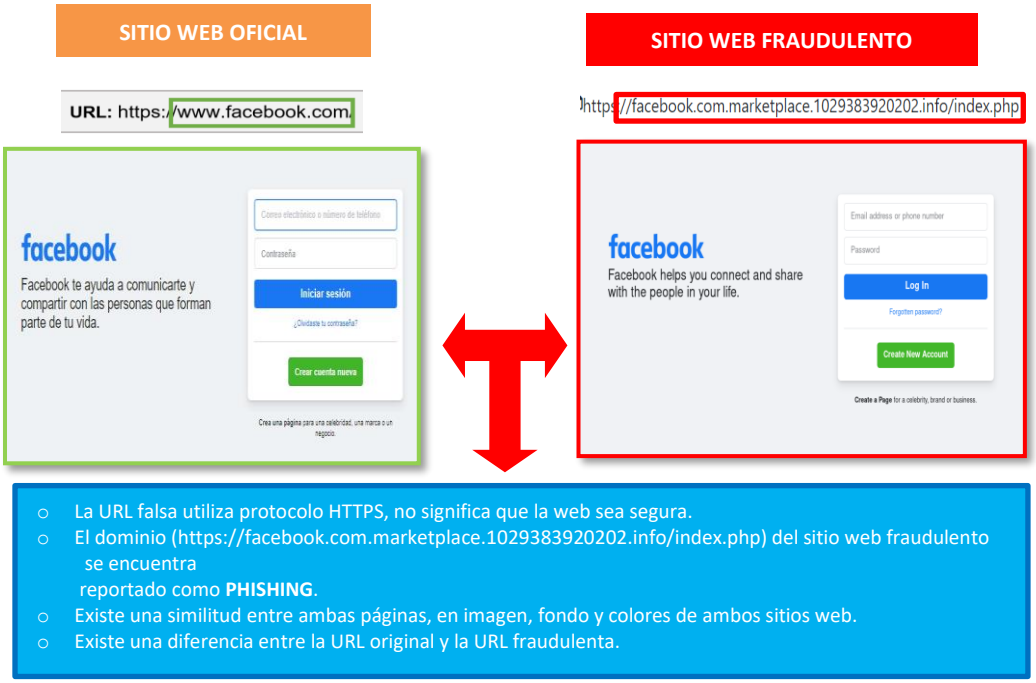


Figura 2. Una vez que el sitio de Phishing ha logrado capturar la dirección del correo electrónico o número de celular como la contraseña. La víctima, es redirigido hacia el sitio oficial de Facebook, aludiendo un aparente error de autenticación.

A. Comparación del sitio web oficial Outlook Web App, con el fraudulento.



- La URL falsa utiliza protocolo HTTPS, no significa que la web sea segura.
- El dominio (https://facebook.com.marketplace.1029383920202.info/index.php) del sitio web fraudulento se encuentra reportado como **PHISHING**.
- Existe una similitud entre ambas páginas, en imagen, fondo y colores de ambos sitios web.
- Existe una diferencia entre la URL original y la URL fraudulenta.

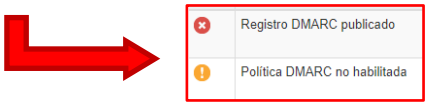
B. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD** en cinco (05), **MALICIOSA** en seis (06) y **MALWARE** tres (03) de ellas- **– PHISHING:**

BitDefender	Malware	CRDF	Malicioso
CyRadar	Malicioso	Emsisoft	Suplantación de identidad
ESET	Suplantación de identidad	Fortinet	Suplantación de identidad
G-datos	Malware	Navegación segura de Google	Suplantación de identidad
kaspersky	Suplantación de identidad	netcraft	Malicioso
Búsqueda segura	Malicioso	Sophos	Malware
VIPRE	Malicioso	raíz web	Malicioso

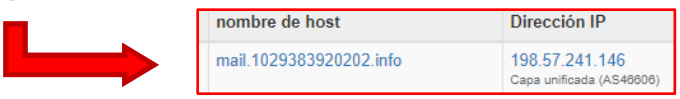
C. Indicadores de compromiso:

- **URL Malicioso:** hxxp://www[.]facebook.com[.]marketplace[.]1029383920202[.]info/index[.]php

- **Dominio:** 1029383920202[.]info

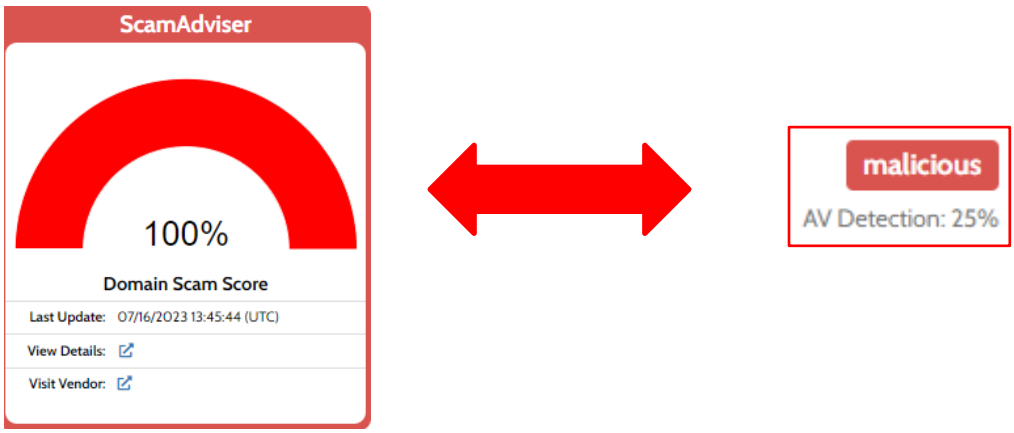


- **Dirección IP:** 198[.]57[.]241[.]146



- **Proveedor de alojamiento:** UNIFIEDLAYER-AS-1

D. Otras detecciones:



3. RECOMENDACIONES:

- Mantener instalado un servicio de antivirus en el dispositivo.
- Verificar la información del sitio web correspondiente.
- Acceder al sitio web a través de fuentes oficiales.
- No abrir enlaces de dudosa procedencia.
- No seguir indicaciones de sitios web fraudulentos.
- No compartir la información con terceras personas, amigos o familiares.

Fuente de Información	Análisis propio de redes sociales y fuente abierta.

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°167	**Fecha: 15-07-2023**
		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 financiero			

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

2. **DETALLES:**

Detalles del proceso de Phishing:

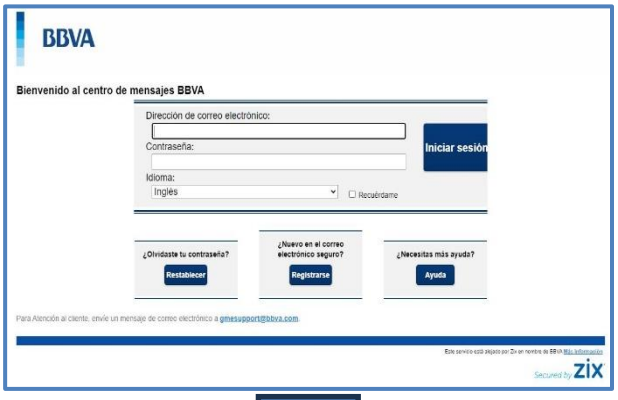


Imagen 1.
Sitio web fraudulenta del Banco BBVA, solicita a las víctimas registrar la dirección del correo electrónico, la contraseña y el idioma para iniciar sesión.

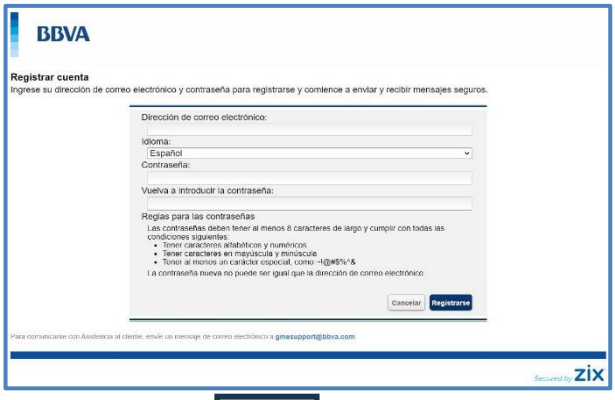


Imagen 2.
Luego de no poder iniciar sesión y darle click en "olvidaste la contraseña" el atacante requiere registrar la dirección del correo electrónico de la víctima, el tipo de idioma y volver a introducir la contraseña para continuar.

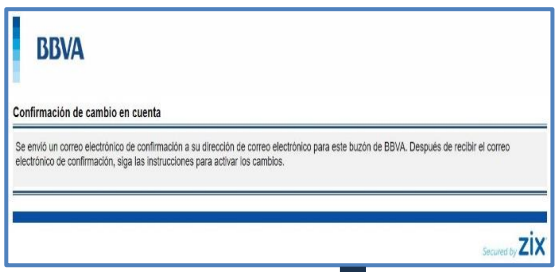
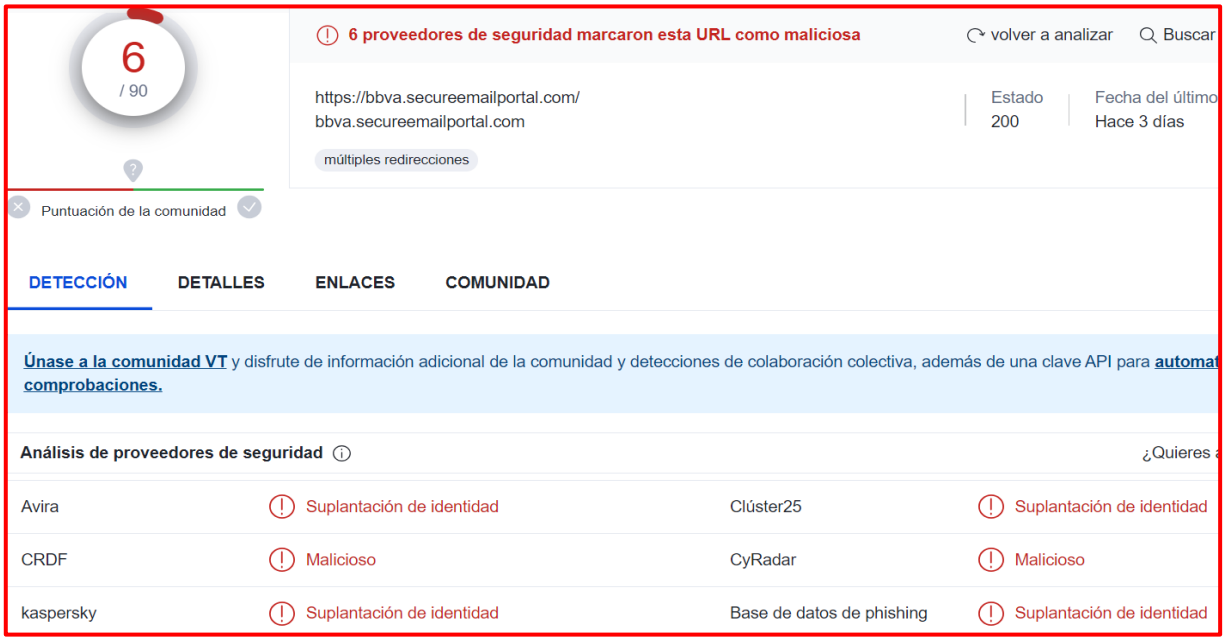
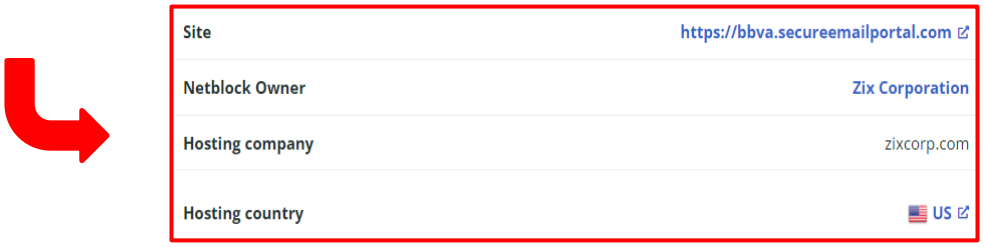


Imagen 3.
Por último, solicita a la víctima confirmar la cuenta, lo cual tendrá que ingresar al correo electrónico y completar lo requerido por los atacantes, para luego informar a la víctima que ha ocurrido un error de autenticación; sin embargo, los datos fueron capturados por los cibercriminales.

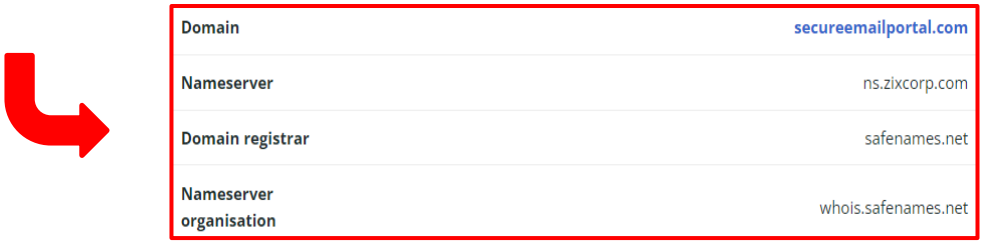
A. Proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD – PHISHING**:



- Indicadores de compromiso:
  - **URL**: hxxps://bbva.secureemailportal.com/



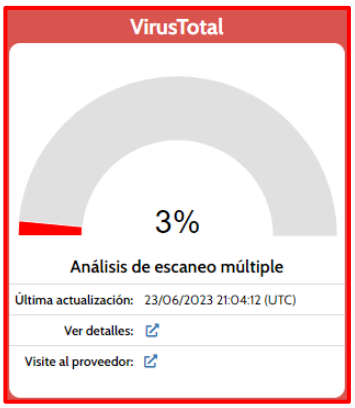
  - **Dominio**: secureemailportal.com



  - **IP**: 199[.]30[.]236[.]16

  - **Server:** Apache
  - **SHA-256**: 9e8a6ec3f9eb1f2dc16f8cc0478ccb596d6a166730536c5dbcd00ecbeb3433a3
  - **Tipo de Contexto:** Text/Html

- **Otros resultados del analisis**:



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 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.

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