	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 152	Fecha: 28-06-2023
		Página 27 de 30

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 Sub familia	G02
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, simulado ser la entidad bancaria BBVA, en cual tiene el objetivo de robar credenciales de acceso, datos personales y/o bancarios.

2. DETALLES:

Proceso de Phishing:

Imagen 1.
Plataforma web fraudulenta del Banco BBVA, solicita a la víctima que se registre digitando el correo electrónico y una contraseña nueva.

Imagen 2.
Después de completar lo requerido por los atacantes, te envían un correo electrónico de confirmación al correo previamente registrado.

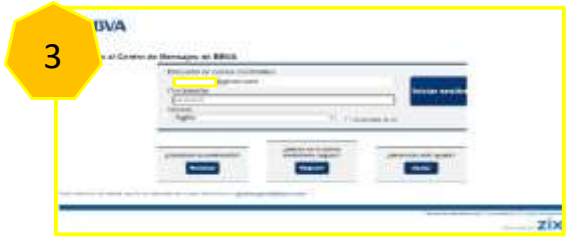


Imagen 3.
Donde al dar siguiente, redirecciona a una pestaña que indica registrar la dirección de correo electrónico y contraseña para el inicio de sesión.

Imagen 4.
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.

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

SITIO WEB OFICIAL	https://www.bbva.pe/
PLATAFORMA WEB FRAUDULENTA	hxxp:// game-eu-message-portal[.]com/s/loginview[.]jsp?b=bbva

- Existe diferencia en el dominio de sitio web fraudulento, no coincide con el oficial.
- El sitio web fraudulento no posee el **PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS)**, lo que hace que no puedan convencer a la víctima, a la hora de ingresar al sitio web.

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

ADMINUSLabs	Malicioso	AlphaSOC	Suplantación de identidad
BitDefender	Malware	CRDF	Malicioso
CyRadar	Malicioso	G-datos	Malware
kaspersky	Suplantación de identidad	Leonico	Malicioso
Búsqueda segura	Malicioso	Sophos	Malware
VIPRE	Malicioso	raíz web	Malicioso
Nube de veredicto de Xcitium	Malicioso	Abusix	Limpio

C. Indicadores de compromiso:

- URL: [.]hxxps://game-eu-message-portal[.]com/s/loginview[.]jsp?b=bbva

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

- Dominio: game-eu-message-portal[.]com

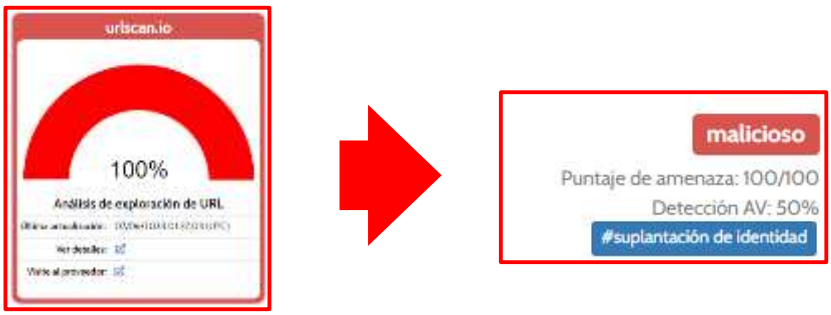
Domain	game-eu-message-portal.com
Nameserver	ns.zixcorp.com
Domain registrar	safenames.net
Nameserver organisation	whois.name.com

- Proveedor de alojamiento: Zix International AG

País: Estados Unidos
Proveedor de alojamiento: Zix International AG
ASN: AS59519
Certificado TLS: Autoridad de certificación de confianza - L1K

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

D. OTRAS DETECCIONES:



3. 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