	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°199		Fecha: 24-08-2023
			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

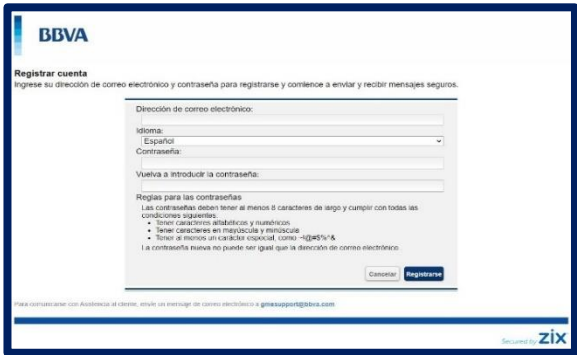
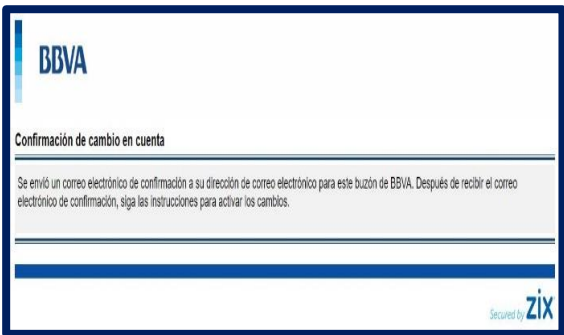


IMAGEN 3:
Por último, solicita a la víctima confirmar la cuenta, lo cual tendría que ingresar al correo electrónico y completar lo requerido por los atacantes, para luego informar a la víctima que ha ocurrido un error de autenticación; sin embargo, los datos fueron capturados por los cibercriminales.



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



Nombre del envío:	hxxps://securemail-bbva.com/s/login?b=bbva
Tamaño:	66B
Tipo:	URL ⓘ
Mímica:	Texto sin formato
Sistema operativo:	ventanas
Último análisis antivirus:	25/09/2021 00:18:26 (UTC)
Último informe de Sandbox:	30/12/2019 21:34:51 (UTC)

II. **SHA-256:** bc2db9b94118ed9f2abaeb0b429905fcd15c91fd1372c9d4a1e3987338a40f3d



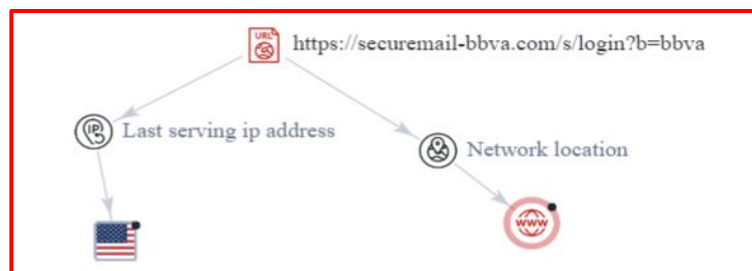
95 (2020_03_15_15_49_50 UTC).descargar	99e60fbdl2fa9c1bb9e 84b4f8fa53169cd9eb 965f08337de199592 6a5ed83f1	🚨 suspicious
buscaramad5fb96dc0cb61b9454244c9bd7fe6_1.js	223cc0c3d2c5e48349 94571da73b15d261a93 d71c03ecb388a993bd 63edd5215	🚨 suspicious
RecoveryStore_888090CO-D917-11E7-B67B-080027A49DD6_dat	423b2e44c97a21b2d7096c25fd05f8d8030a4c25b3f6aafed1db3d25b51e02 3	✅ no specific threat

III. **IP:** 207[.]195[.]182[.]115



Connection		Detection	
Representative Domain	N/A	Proxy IP	False
SSL Certificate	🚨 True (web1.zixmail.net)	VPN IP	False
IP Address Owner	ASN-CUST	Tor IP	False
Hostname	Mailerdal-rys-rv.zixmessagecenter.com	Hosting IP	False
Connected Domains	🚨 19	Mobile IP	False
Country	🇺🇸 United States	CDN IP	False
		Scanner IP	False
		Special Issue	0

IV. **Tipología:**




Se puede apreciar 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:

MALICIOSO

 <https://securemail-bbva.com/s/...>


Analizado en: 30/12/2019 21:34:51 (...)

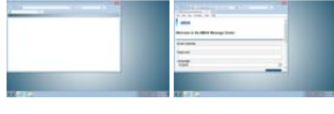
Ambiente: windows 7 32 bits

Puntuación de amenaza: 50/100

Detección AV: 2% sitio de phishing

Indicadores: 2 4 14

Red: 





malicioso

Puntuación de amenaza: 50/100

Detección AV: 1%

Etiquetado como: Sitio malicioso

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.

3. 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.
- Introduce 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.