

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°002		Fecha: 02-01-2024
			Página: 5 de 8
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Phishing, suplantando la identidad del Banco "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:

Hola, introduce tu usuario y clave de acceso y entra en BBVA online para activar:

NIF, NIE, Pasaporte o Tarjeta Anónima

¿Olvidaste tu contraseña?

IMAGEN 1:

Plataforma web fraudulenta del Banco BBVA, solicita a la víctima datos personales, tales como introducir el usuario (NIF, NIE, PASAPORTE O TARJETA ANÓNIMA) y la clave de acceso.

IMAGEN 2:

Una vez ingresado los datos, el atacante requiere que registre su correo electrónico para poder continuar.

¡Bienvenido!

Ingresar tu correo electrónico registrado

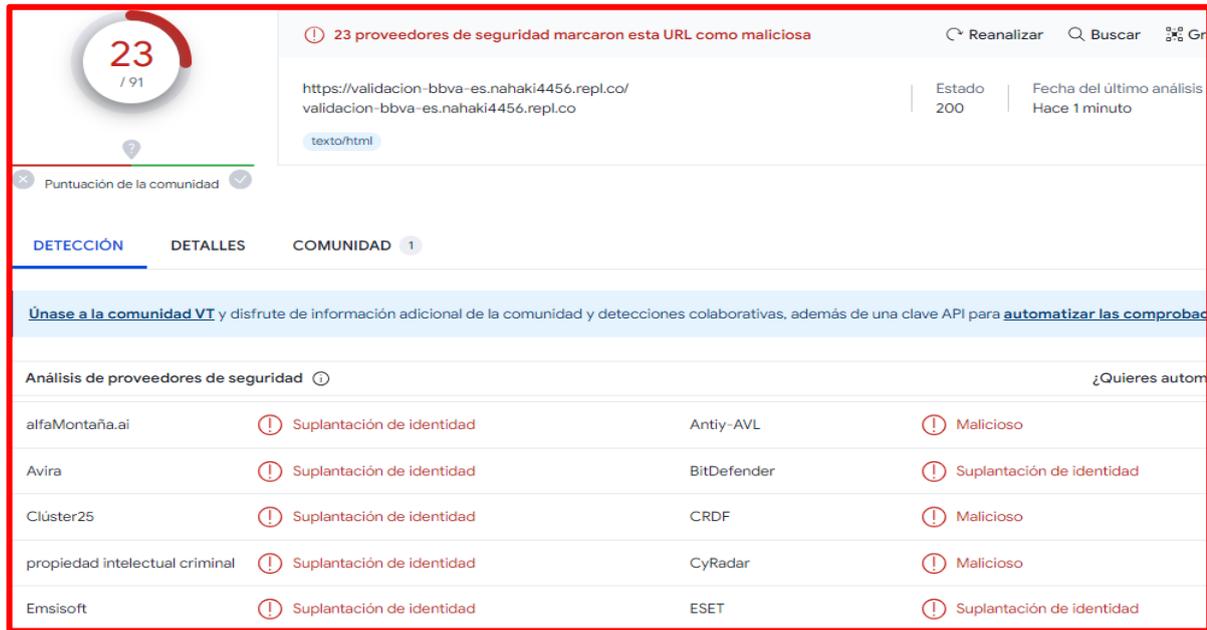
¡Bienvenido!

Ingresar el código sms recibido para validar su titularidad

IMAGEN 3:

Luego, le envía el código al correo electrónico para validar su titularidad y completar lo requerido por los atacantes, al continuar 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. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**



23 / 91

23 proveedores de seguridad marcaron esta URL como maliciosa

Reanalizar | Buscar | Gr

https://validacion-bbva-es.nahaki4456.repl.co/validacion-bbva-es.nahaki4456.repl.co

Estado: 200 | Fecha del último análisis: Hace 1 minuto

texto/html

Puntuación de la comunidad

DETECCIÓN | DETALLES | COMUNIDAD 1

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	Alerta	Detalles
alfaMontaña.ai	Suplantación de identidad	Antiy-AVL	Malicioso	
Avira	Suplantación de identidad	BitDefender	Suplantación de identidad	
Clúster25	Suplantación de identidad	CRDF	Malicioso	
propiedad intelectual criminal	Suplantación de identidad	CyRadar	Malicioso	
Emsisoft	Suplantación de identidad	ESET	Suplantación de identidad	

a) Indicadores de compromisos:

I. URL: hxxps://validacion-bbva-es[.]nahaki4456[.]repl[.]co/



Site	https://validacion-bbva-es.nahaki4456.repl.co
Netblock Owner	Google LLC
Hosting company	Google
Hosting country	US

II. DOMINIO: repl[.]co



Domain	repl.co
Nameserver	ns1.replit.com
Domain registrar	nic.co
Nameserver organisation	whois.cloudflare.com

III. IP: 35[.]186[.]245[.]55



IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
35.0.0.0-35.255.255.255	United States	NET35	American Registry for Internet Numbers
35.184.0.0-35.191.255.255	United States	GOOGLE-CLOUD	Google LLC
35.186.245.55	United States	GOOGLE-CLOUD	Google LLC

B. Otras detecciones:

MALICIOUS

 <https://validacion-bbva-es.naha...>

Analyzed on: 12/29/2023 16:13:54 (UTC)

Environment: Windows 10 64 bit

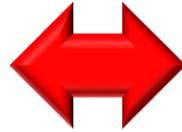
Threat Score: 100/100

AV Detection: 20% Phishing site

Indicators: 2 4 9

Network: 





malicioso

Puntuación de amenaza: 100/100

Detección AV: 26%

#suplantación de identidad

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 envío 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, mensajes de textos - SMS, etc.

D. Referencia:

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.
- Introducir 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.
------------------------	---