	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°187	Fecha: 10-08-2023
		Página: 9 de 12

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:

IMAGEN 1:

Plataforma web fraudulenta del Banco BBVA, solicita a la víctima datos personales, tales como (nombre y apellidos, documento de identidad - DNI, clave de acceso y número telefónico.

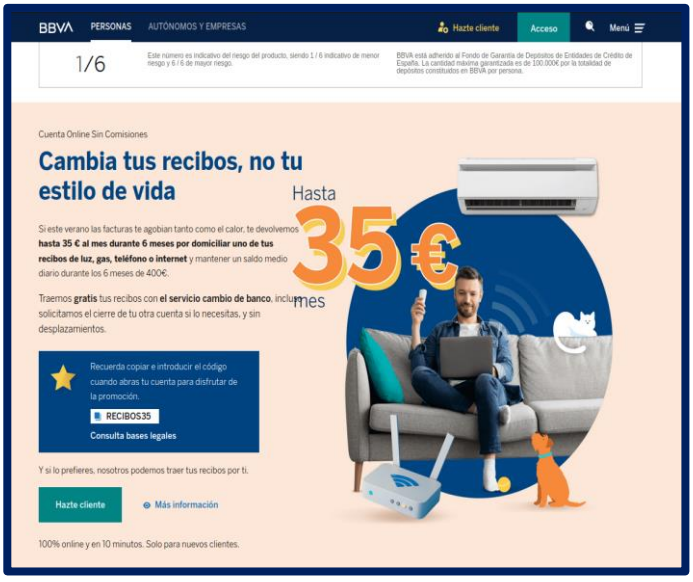


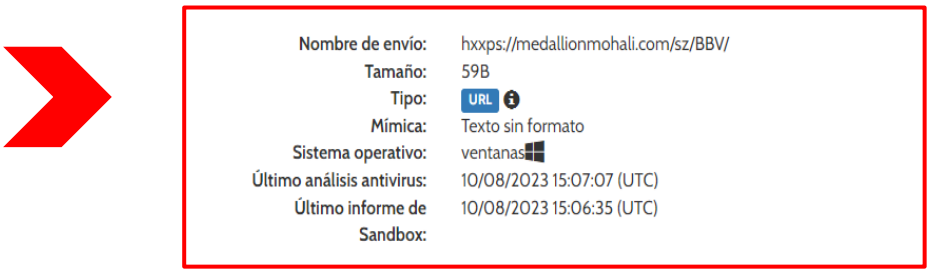
IMAGEN 2:

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. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

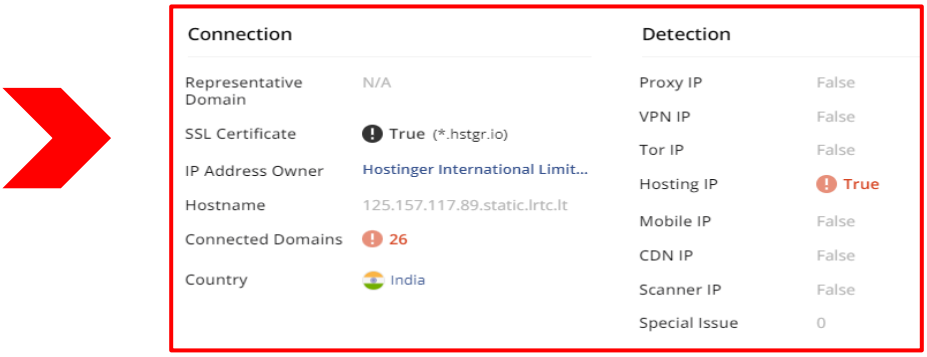
Indicadores de compromisos:

I. URL: hxxps[:]//medallionmohali[.]com/sz/BBV/



II. SHA-256: 86100d37c9191524370ee7d46d44a08b0ed8f0ef45c2d3f5bf63a598465ac3b5

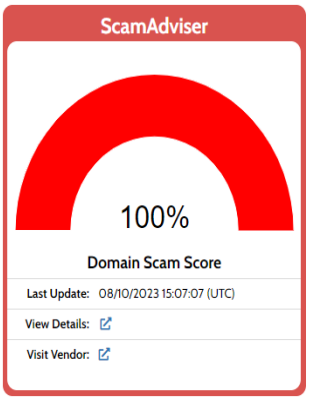
III. IP: 89[.]117[.]157[.]125

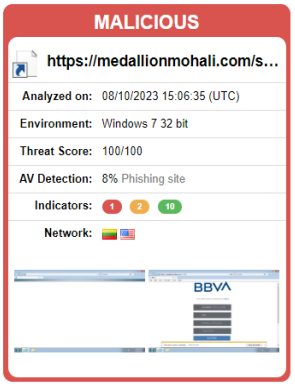


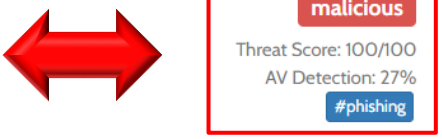
B. Se hallaron **08 proveedores** de seguridad que marcaron este dominio como malicioso.

Avira	Phishing	BitDefender	Phishing
Fortinet	Phishing	G-Data	Phishing
Lionic	Phishing	Sophos	Phishing
Trustwave	Phishing	Webroot	Malicious

C. Otras detecciones:







D. 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, mensajes de textos - SMS, etc.

E. 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.