	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 071	**Fecha: 12-03-2022**
		Página 3 de 5

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de Alerta	Nueva campaña de Smishing que suplanta la identidad del BBVA.		
Tipo de Ataque	Suplantación	Abreviatura	Suplantación
Medio de Propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Subfamilia	G03
Clasificación temática familia	Fraude		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de propagación de mensajes de texto falsos (Smishing), a teléfonos móviles, que aparenta provenir del Banco BBVA, donde advierte sobre: "***Un dispositivo no autorizado se ha conectado a su cuenta online. Si no reconoce este acceso verifique ahora***", adjunto un enlace que redirige a un sitio web falso similar al Oficial de la Banca por Internet del BBVA, con el objetivo robar credenciales de acceso, datos personales y bancarios.

2. Proceso del ataque phishing:

Imagen 01: Mensaje de texto aparentemente enviado del Banco BBVA, advierte sobre ***"Un deposito no autorizado"***, para verificar solicita a la víctima, ingresar en el enlace adjunto.

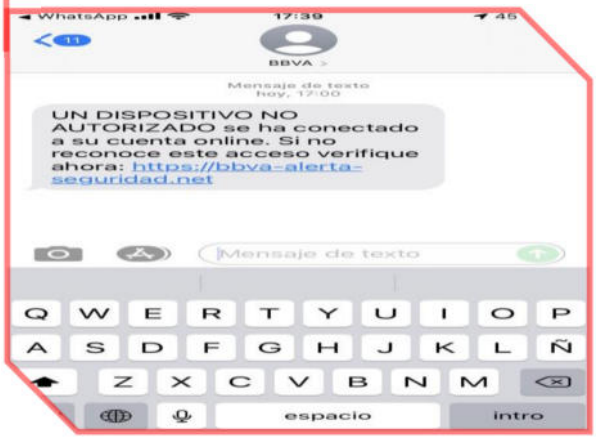

Imagen 02: Una vez hecho clic, en el enlace, es redirigido a un sitio web falso similar a la Banca por Internet del BBVA, donde solicita ingresar las credenciales de acceso (NIF, NIE, Tarjeta, Pasaporte y clave web).

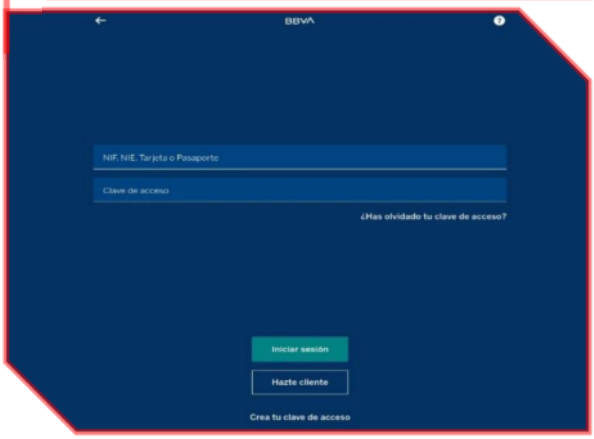

Imagen 03: Luego, de haber hecho clic, en <Iniciar sesión>, requiere ingresar el número de teléfono asociado a la cuenta, y "Confirmar".

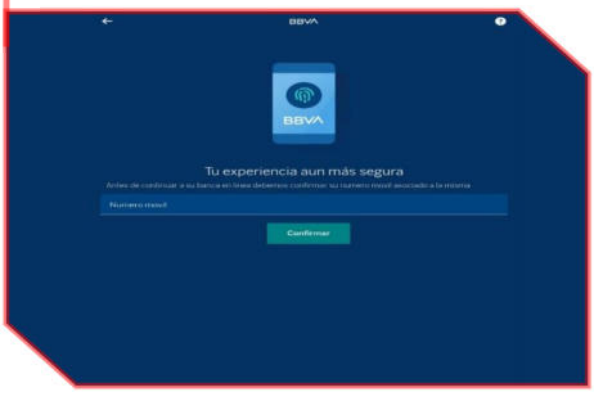

Imagen 04: Pasado unos 20 segundos, es redirigido al sitio web oficial del Banco BBVA, aludiendo un aparente error de autenticación; sin embargo, los datos fueros capturados por los ciberdelincuentes.

3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultado lo siguiente:
   - Indicadores de compromiso:
     - URL: hXXps[:]//bbva-alerta-seguridad[.]net/
     - Dominio: bbva-alerta-seguridad[.]net
     - Dirección IP: 104[.]21[.]4[.]131
     - Código: 404
     - SHA-256: 09b0a1c0fa33fcc8e1d6b8ed59dc9d1e

4. Otras detecciones:
   - URL: hXXps[:]//bbva-alerta-seguridad[.]net/

5. Cómo funciona el Smishing:

   - Los mensajes enviados a las víctimas, finge ser emitido por un banco, comercios u organismos gubernamentales alertando una situación de urgencia u oportunidad.
   - Los mensajes contienen enlace que proporcionan más información o soluciones.
   - Los mensajes vienen desde un número de celular de orígenes desconocidos o anónimos

6. Referencia:

   - El Smishing es una técnica que consiste en el envío de un SMS por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.), con el objetivo de robar información privada o realizarle un cargo económico. Generalmente el mensaje invita a llamar a un número de teléfono o acceder a un enlace de una web falsa bajo un pretexto.

7. Recomendaciones:

   - Evitar acceder a enlaces que forman aparte de un contenido de mensajes texto.
   - Evitar proporcionar información confidencial por teléfono, WhatsApp, mensaje de texto, correo electrónico o redes sociales, a través de enlaces.
   - Verificar la procedencia de los mensajes texto, en fuentes oficiales de la entidad que provee algún servicio o producto.
   - Contar con una solución de seguridad, constantemente actualizada tanto en dispositivos de escritorio como en móviles, ya que sirven como barrera inicial protectora ante sitios web maliciosos.

Fuente de Información	Análisis propio de redes sociales y fuente abierta