	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 289	Fecha: 24-10-2022
		Página 05 de 08

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Campaña de phishing que tiene como objetivo robar credenciales de acceso, datos personales y/o bancarios 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 subfamilia	G02
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 phishing "tipo de robo de identidad en línea", que utilizando correos electrónicos falsos suplanta la identidad del banco BBVA, para atraer la atención de la víctima, en el texto del mensaje se advierte que ***"¡Tu servicio del BBVA-APP ha caducado!",*** por lo que será cancelada a menos que se ingrese en ***"Acceder a mi cuenta",*** para actualizar la información, con el objetivo robar credenciales de acceso, datos personales y/o bancarios.

2. Proceso del ataque phishing:

Imagen 1: Correo electrónico que suplanta la identidad del banco BBVA, incita a la víctima, hacer clic en ***<< Acceder a mi cuenta>>.***

Imagen 2: Solicitud para ingresar (cedula de ciudadanía, numero de documento y contraseña)

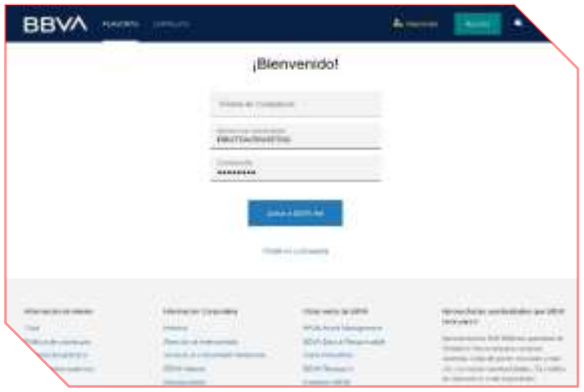
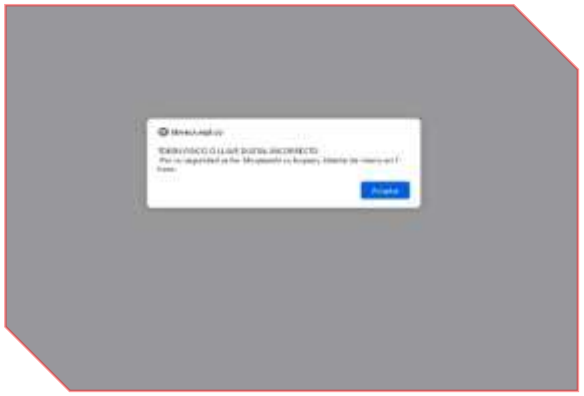


Imagen 3: Engaño, ingresar el código de confirmación enviado al buzón de notificación en BBVA móvil, para finalizar la verificación de identidad.

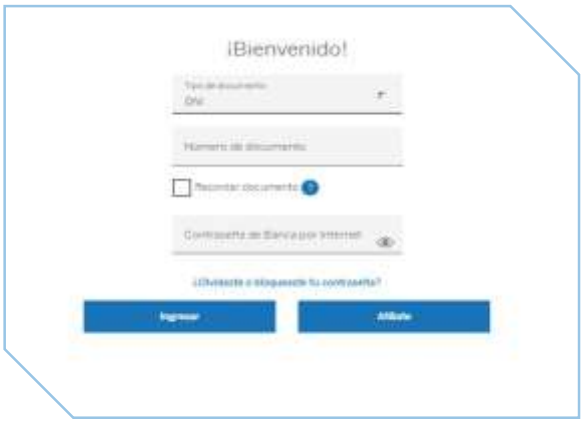
Imagen 4: Aviso ***"Token o llave digital incorrecto",*** aludiendo un aparente error, indicando que se ha bloqueado la cuenta y que intente más luego; Sin embargo, los datos fueron capturados por los ciberdelincuentes



3. Comparación de sitio web oficial BBVA y sitio web falso:

SITIO OFICIAL
URL: https://www.bbva.pe/

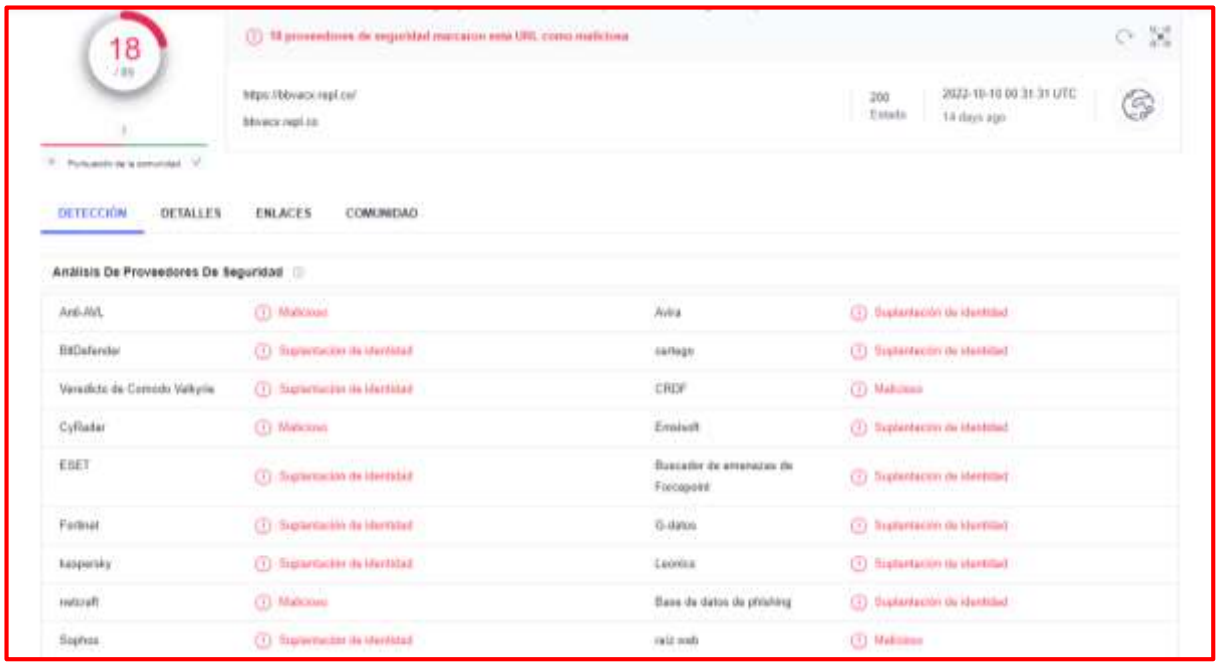
SITIO FRAUDULENTO
URL: hXXps[:]//bbvacx[.]repl[.]co/



- Existe similitud en imagen de fondo, color y escritura.
- Tiene certificado de seguridad de protocolo HTTPS.
- El dominio se hace pasar por el sitio oficial, pero no coincide.

4. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo la siguiente información:

- **URL:** hXXps[:]//bbvacx[.]repl[.]co/
- **Dominio:** bbvacx[.]repl[.]co
- **Direcciones IP:** 34[.]149[.]204[.]188
- **Código De Estado:** 200
- **Tamaño:** 268.24 KB
- **SHA-256:** 832e5b6141d0b025ead4772da2bdb6403b5bd02adb210e0ca2972c650e2e1b9c



5. **Otras detecciones del análisis**:

6. **Recomendaciones:**

- Acceder al sitio web a través de fuentes oficiales
- Evitar responder a mensajes enviados desde (correo electrónico, Whatsapp, SMS y otros), que contengan enlaces de dudosa procedencia.
- Verificar detenidamente la redacción y ortografía de la dirección URL, que coincidan con el sitio web oficial.
- Evitar proporcionar información personal y/o financiera a través de sitios webs de dudosa procedencia.
- Utilizar una firma de antivirus actualizado, ya que es la primera barrera ante posibles ataques cibernéticos.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta