	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 015	Fecha: 15-01-2022
		Página: 5 de 7

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**			
Nombre de la alerta	Nueva campaña de phishing dirigidos a usuarios 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 subfamilia	G02	
Clasificación temática familia	Fraude Financiero			

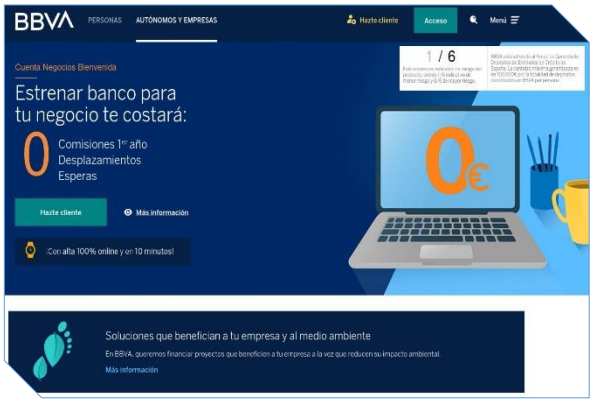
Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los cibercriminales vienen realizando avanzados ataques de phishing que se distribuye a través de navegadores web, suplantando la identidad de la Banca online de BBVA, con el objetivo robar credenciales de acceso, datos personales y bancarios vinculados a la cuenta de la víctima.

2. Proceso del ataque phishing:

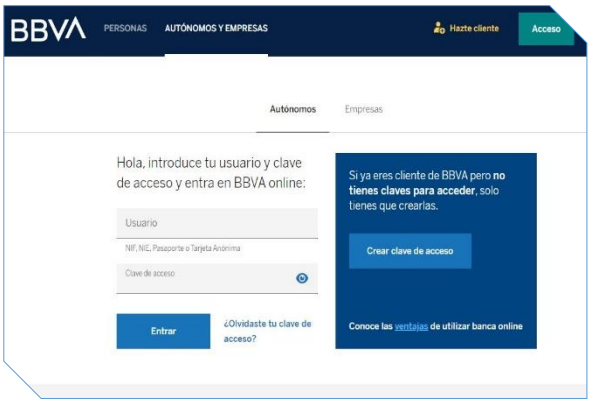
Figura N° 01: Sitio web falso que suplanta la identidad de la Banca Online de BBVA, solicita al usuario ingresar sus credenciales de acceso (usuario y clave web).

Figura N° 02: Pasado unos segundos, es redirigido al sitio web oficial del Banco BBVA, aludiendo un aparente error de autenticación, sin embargo, los datos fueron capturados.



3. Comparación del sitio oficial de la Banca Online BBVA con sitio fraudulento:

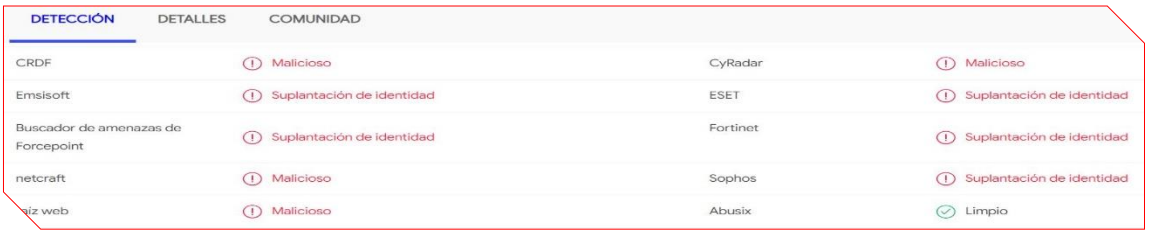
Sitio oficial
URL: https://www.bbva.es/empresas.html



Sitio fraudulento
URL: hXXps[:]//bkkonline[.]sumbarprov[.]go[.]id/bbva/

El sitio falso utiliza las imágenes, colores, formatos y tipografías con finalidad que la víctima crea que se encuentra en la web oficial del Banco BBVA. La diferencia se encuentra en la URL.

4. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultados que, NUEVE (09) proveedores de seguridad informática alertan como **PHISHING.**
   - URL Final: https[:]//bkkonline[.]sumbarprov[.]go[.]id/bbva/
   - Dominio: bkkonline[.]sumbarprov[.]go[.]id
   - Dirección IP: 103[.]160[.]118[.]10
   - Código De Estado: 200
   - Longitud Corporal: 1.05KB
   - Cuerpo SHA-256: 6bf154ee15366c533a5532827e1e91cbf37b2a0e27ced10c47ef4b8913889d31



5. Otras detecciones:
   - Dirección web: https[:]//bkkonline[.]sumbarprov[.]go[.]id/bbva/

   - Lista negra: Bkkonline[.]sumbarprov[.]go[.]id

6. Recomendaciones:
   - Asegurarse que la página a la que intentas ingresar sea el sitio oficial de tu entidad bancaria.
   - Actuar con precaución al seguir enlaces o descargar ficheros adjuntos en correos electrónicos, SMS, mensajes en WhatsApp o redes sociales, aunque sean de contactos conocidos.
   - Evitar guardar información bancaria en el dispositivo móvil.
   - Verificar la fuente de información de tus correos entrantes.
   - Asegurarse de contar con un antivirus instalado en su equipo y que este se encuentre debidamente actualizado.

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