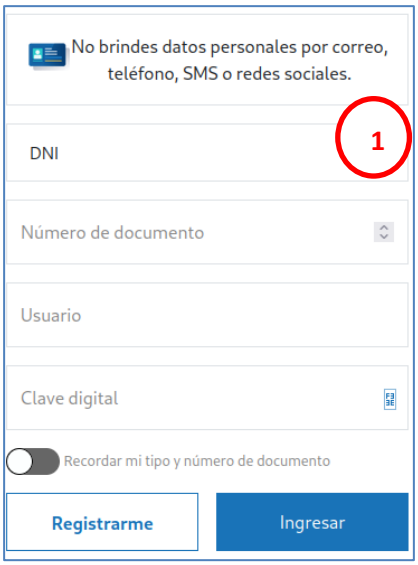
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 090	Fecha: 17-04-2023
		Página 6 de 10

Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Campaña de 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 subfamilia	G02
Clasificación temática familia	Fraude		

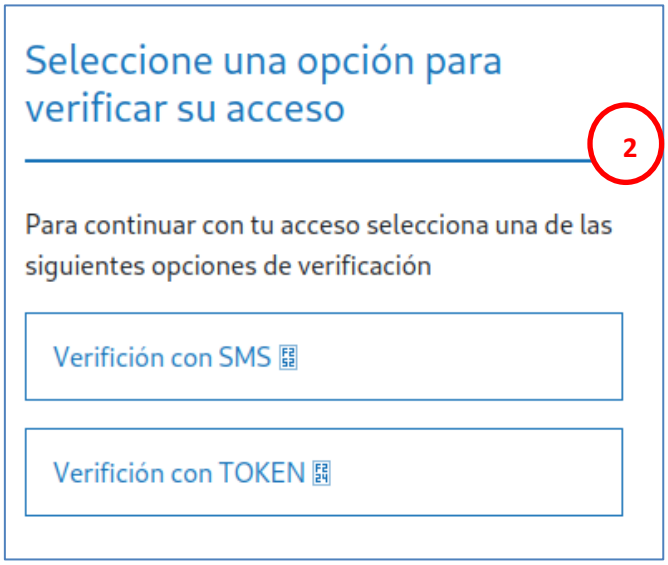
Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo avanzados ataques cibernéticos, por medio de envíos masivos de correos electrónicos fraudulentos, o también conocidos como Phishing, simulando ser la página oficial del Banco BBVA, requiriendo a las víctimas ingresar las credenciales de inicio de sesión como número de DNI, usurario y clave digital de la cuenta, a fin de realizar una verificación de acceso a la misma.

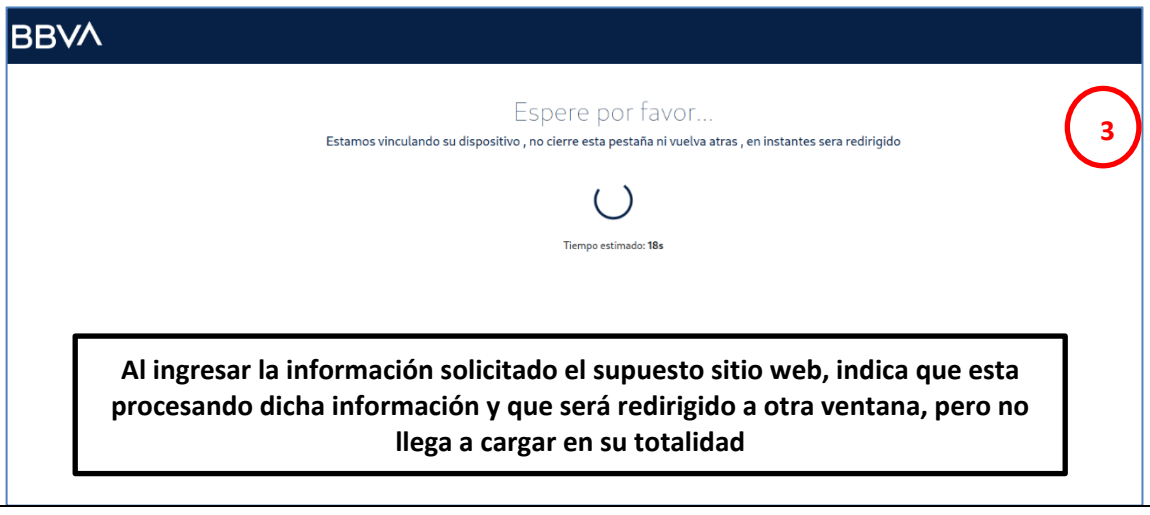
2. Detalles del proceso de Phishing:



Requiere ingresar las credenciales de inicio de sesión

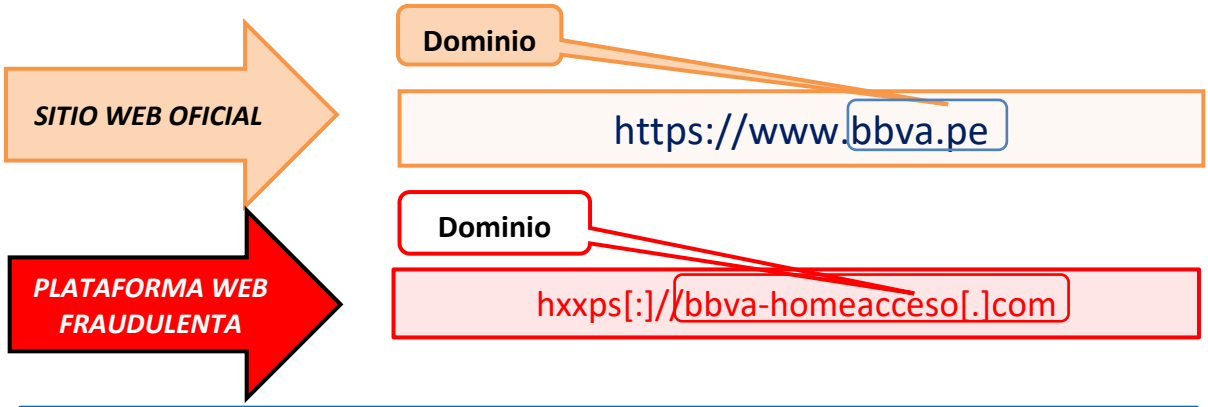


A fin de verificar el acceso a la cuenta bancaria, pide elegir el método de verificación



Al ingresar la información solicitado el supuesto sitio web, indica que esta procesando dicha información y que será redirigido a otra ventana, pero no llega a cargar en su totalidad

3. Comparación del sitio web oficial y sitio web fraudulento del Banco BBVA:



- Existe diferencia entre los dominios del sitio web oficial y fraudulento.
- Ambos sitios web poseen el **PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS),** lo cual hace más convincente a la que las víctimas ingresen a dicho sitio web.

4. Proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD – PHISHING:**

alphaMountain.ai	Phishing	Avira	Phishing
CRDF	Malicious	CyRadar	Malicious
ESET	Phishing	Forcepoint ThreatSeeker	Phishing
Fortinet	Phishing	Sophos	Malware
Trustwave	Phishing	Abusix	Clean

- Indicadores de compromiso:
  - URL: hxxps[:]//bbva-homeacceso[.]com
  - Dominio: bbva-homeacceso[.]com
  - SHA-256: 9a50136a82e60c31374c9e33aa75b51a291d26b5c0a4f118063b801ff11da9c0
  - Dirección IP: 172[.]67[.]135[.]191
  - Tamaño: 3.84 KB

5. Recomendaciones:

- Comunicarse con la entidad, a fin de corroborar la información solicitada.
- Verificar detalladamente la URL, que corresponda al sitio web oficial.
- Ingresar desde fuentes oficiales.
- Evitar seguir las instrucciones de sitio web sospechoso o de dudosa procedencia.
- Mantener el antivirus actualizado, ya que es la primera barrera ante posibles ataques cibernéticos.
- Evitar compartir la URL con amigos y/o familiares.

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

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 090	Fecha: 17-04-2023
		Página 8 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de falso servicio del correo electrónico de Microsoft.		
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 actores de amenazas vienen realizando una campaña de Phishing, activando un falso servicio del correo electrónico de la compañía Microsoft (Outlook, Hotmail, etc.), con la finalidad de obtener las credenciales de acceso (correos y contraseñas) de los usuarios de la compañía tecnológica.

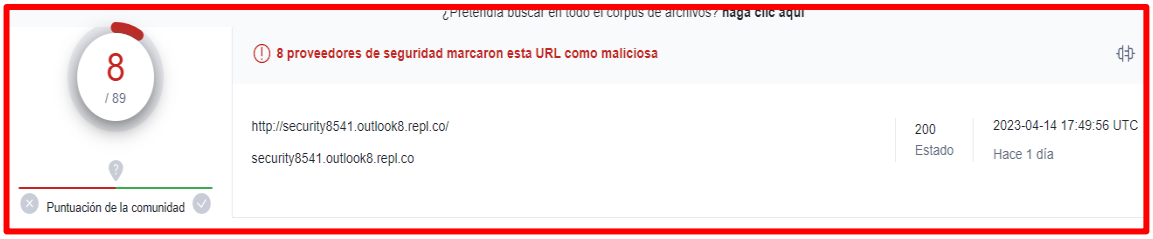
2. **Detalles del proceso de Phishing**

EL ATACANTE SOLICITA A LA VÍCTIMA QUE REGISTRE EL CORREO ELECTRÓNICO y CONTRASEÑA, PARA ACCEDER AL SERVICIO EN LA WEB DE LA COMPAÑÍA MICROSOFT (OUTLOOK, HOTMAIL, ETC.)

AL INICIAR SESIÓN, EL ATACANTE REQUIERE COLOCAR UN PIN DE CUATRO DIGITOS, CON LA FINALIDAD DE OBTENER UNA MAYOR ACCEBILIDAD PARA INGRESAR AL CORREO ELECTRONICO.

AL COMPLETAR LO REQUERIDO, LE REDIRIGE AL SITIO OFICIAL DEL SITIO WEB DE MICROSOFT, ALUDIENDO UN APARENTE ERROR DE AUTENTICACIÓN; SIN EMBARGO, LOS DATOS FUERON CAPTURADOS POR LOS CIBERCRIMINALES

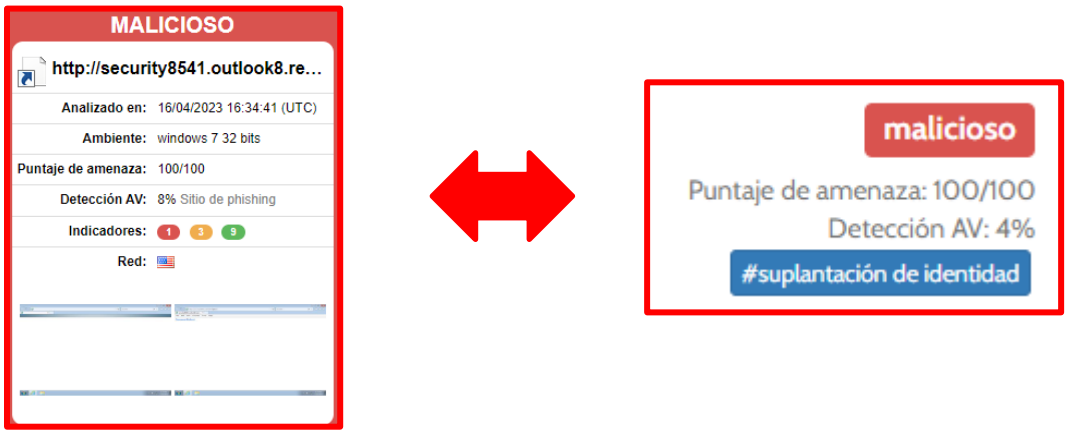
3. **Proveedores de seguridad informática alertan como SUPLANTACIÓN DE IDENTIDAD - PHISHING.**



4. **Indicadores de compromiso (IoC)**

- ✓ URL : hxxps://security8541[.]outlook8[.]repl[.]co/
- ✓ Dominio : repl.co
- ✓ Tipo : text/html
- ✓ Tamaño : 1.28 KB
- ✓ SHA-256 : cf02cc24fa5821e6bc302c1a0dc1d646a1053a0ff2bb8ec25ec111b2acd56ac7
- ✓ IP : 34[.]149[.]204[.]188

5. **Otras detecciones:**



6. **Apreciación de la información:**

- La presente campaña de Phishing permite a los actores de amenazas obtener las credenciales de acceso del servicio del correo electrónico en la web de la compañía Microsoft (Outlook, Hotmail, etc.).

- 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, dicho enlace malicioso, es enviado a través de las plataformas digitales como el WhatsApp, Telegram, Messenger y mensajes de textos SMS.

7. **Algunas Recomendaciones**:

- Verificar detalladamente las URL de los sitios web
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.
- Descargar aplicaciones de fuentes confiables.
- Realizar las actualizaciones correspondientes desde fuentes originales.

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