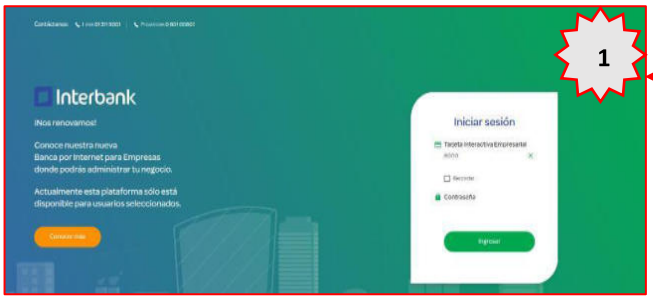
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 064	**Fecha: 05-03-2022**
		Página 7 de 9

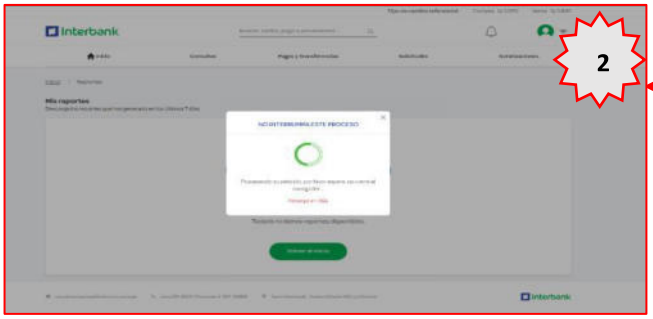
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de Alerta	Campaña de Phishing, suplantando la identidad del Banco Interbank		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medio de Propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Subfamilia	G02
Clasificación temática familia	Fraude		

Descripción

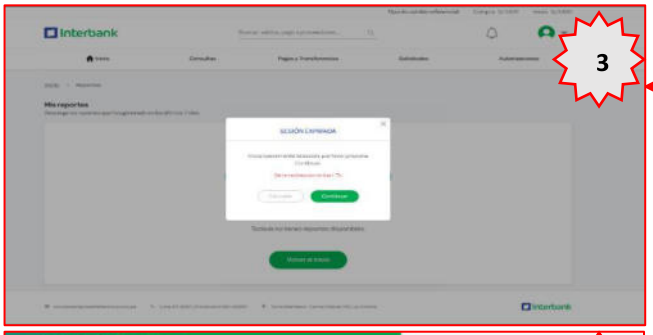
1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de Phishing, por medio de los diferentes navegadores web, dirigido a los clientes y/o usuarios del Banco **INTERBANK**; el cual, mediante la creación de un supuesto sitio web "**Banca Por Internet**" de la entidad bancaria, solicitan a las posibles víctimas a ingresar las credenciales de inicio de sesión, como número de tarjeta y clave web, con la finalidad de apoderarse de manera ilícita de la información bancaria.
2. **Imagen**: Detalle del proceso del Phishing:



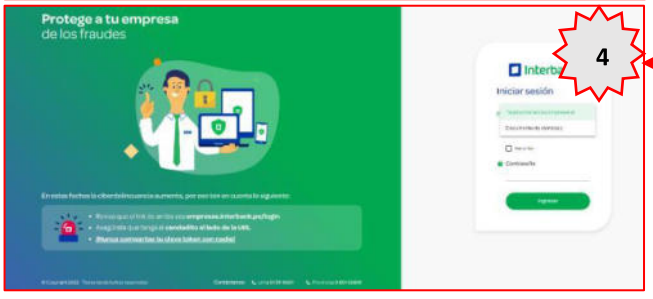
Solicitan a las posibles víctimas ingresar datos confidenciales, como Número de tarjeta y clave web.



Indica que el supuesto sitio web está procesando la información, sugiriendo no cerrar el navegador, no llegando a procesar al 100%.



Después de un determinado tiempo, a través de una ventana emergente indica que la sesión ha expirado, solicitando hacer clic en continuar para iniciar sesión nuevamente.



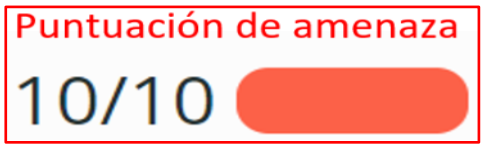
Por último, redirige automáticamente al sitio web oficial del Banco Interbank, aludiendo un aparente error de autenticación; sin embargo, los datos ingresados fueron capturados por los ciberdelincuentes.

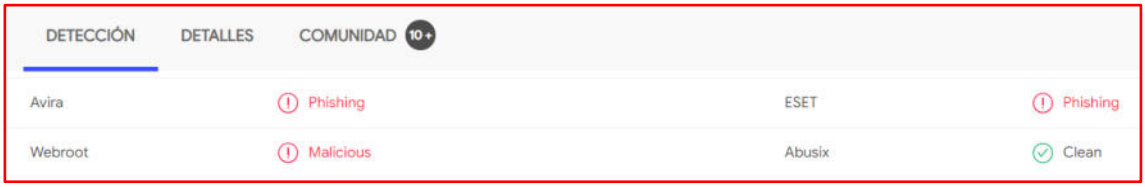
3. Comparación del sitio web oficial y fraudulento.

- Existe una similitud entre el fondo y forma de cada sitio web.
- Ambas URL´s utilizan el protocolo HTTPS, lo que hace más convincente a que las víctimas accedan al sitio web.
- La diferencia está en la URL, debido a que el dominio del sitio web fraudulento no coincide con el oficial.

4. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como Phishing (suplantación de identidad):

- Indicadores de compromiso:
  - URL: hxxps[:]//xn--intenbnk-eza.xn--emprass-gya[.]com
  - Dominio: xn--emprass-gya[.]com
  - IP: 104[.]21[.]23[.]139
  - Tamaño: 69B
  - SHA-256: 52e6d7e855244f2f876be6a41ea3ca7da235d9b7406fb3bf27bff6194ce93e2f





5. Apreciación de la información:

- La presente campaña de Phishing, permite a los actores de amenazas obtener información bancaria de los usuarios del Banco Interbank
- 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.

6. Referencia.

- PHISHING: Es un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar.

7. Recomendaciones:

- No brindar información personal y/o bancaria en sitios web de dudosa procedencia.
- Ingresar de forma manual la URL de la entidad correspondiente.
- Verificar la información en la entidad correspondiente.
- No compartir la información con familiares o amigos.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener un software antivirus.

Fuente de Información	Análisis propio de redes sociales y fuente abierta