	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 123	Fecha: 05-05-2022
		Página 8 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Smishing, Campaña de envió de SMS fraudulentos, suplantando la identidad del banco Interbank.		
Tipo de ataque	Smishing	Abreviatura	Smishing
Medios 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 diferentes delitos informáticos empleando la modalidad "Smishing" (SMS), quienes suplantan la identidad del Banco Interbank, indicando que el cliente cuenta con un depósito de S/. 210.00 correspondiente al Bono Subsidio, para ello se quiere ingresar a un link adjuntado en el mensaje enviado.

2. **Imagen**: Detalle del proceso del Smishing:

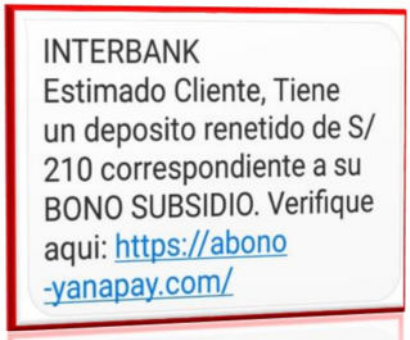


Imagen 1: Mensaje enviado a la víctima.

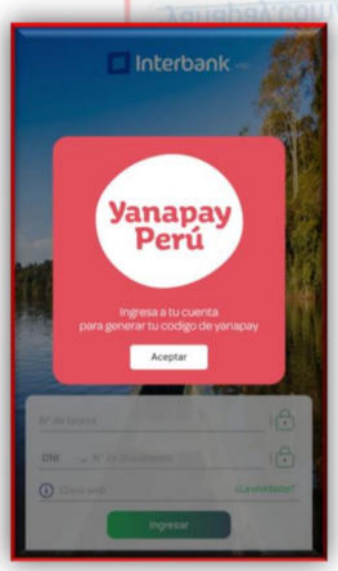


Imagen 2: Una vez hecho clic, en el enlace del mensaje, es redirigido a un sitio falso que suplanta la identidad del Banco Interbank, con el fondo de Yanapay Perú.

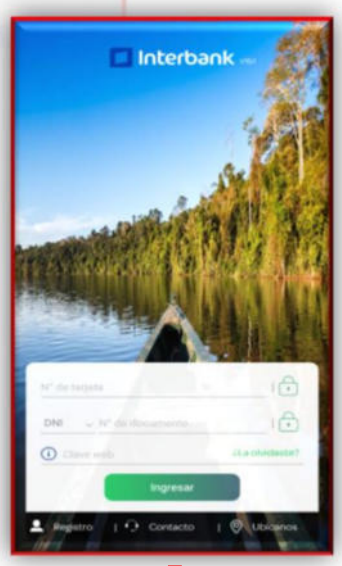


Imagen 3: Sitio web falso, donde requiere el ingreso de las credenciales de acceso (número de tarjeta, DNI y clave web).

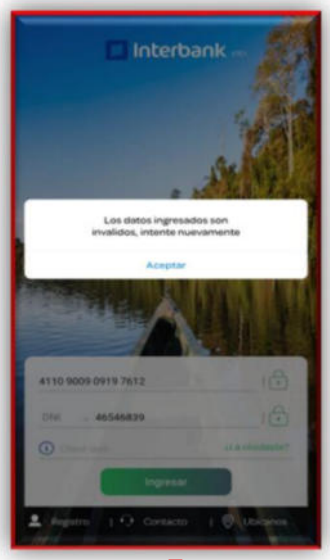
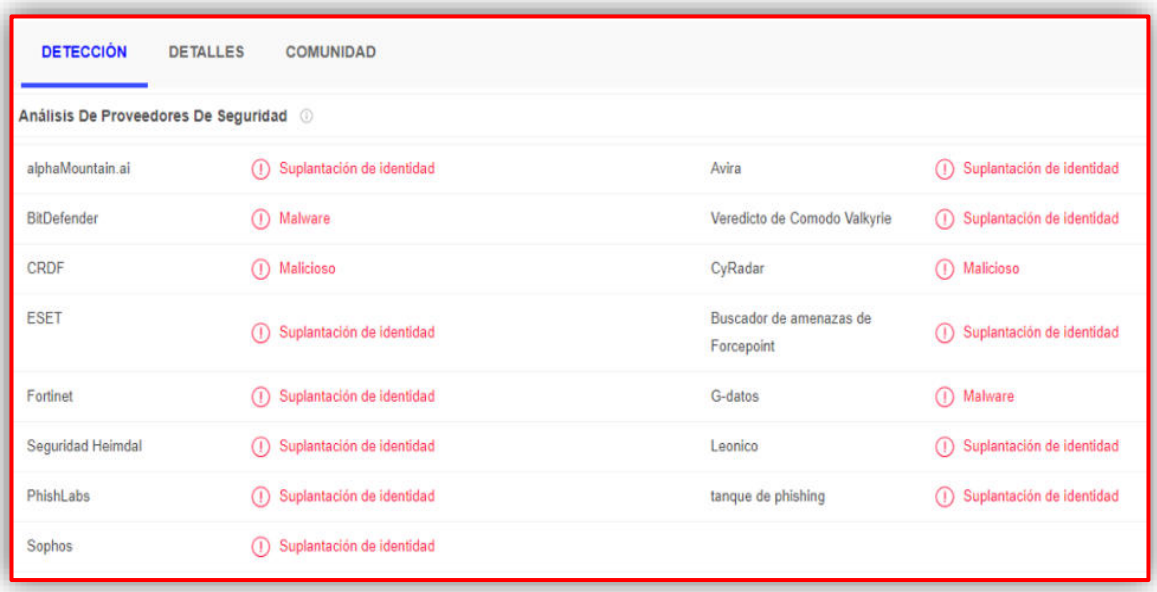


Imagen 4: Pasado unos segundos, aparece un mensaje indicando "Los datos ingresados son inválidos, intente nuevamente", aludiendo un aparente error de autenticación, sin embargo, los datos fueron capturados.

3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

- **INDICADORES DE COMPROMISO:**

  - ✓ **URL:** hxxps://abono-yanapay[.]com/
  - ✓ **Dominio:** abono-yanapay[.]com
  - ✓ **IP:** 45[.]13[.]252[.]188
  - ✓ **SHA-256**: 2c578007dfbc320d7e6358bb8f3b9be343487b64130d69259b94eb3b1d3e7162



- **OTRAS DETECCIONES:**

4. **ALGUNAS RECOMENDACIONES:**

- Verificar la información en la entidad correspondiente.
- Acceder al sitio web a través de fuentes oficiales.
- No abrir enlaces de dudosa procedencia.
- No seguir indicaciones de sitios web fraudulentos.
- No compartir la información con terceras personas, amigos o familiares.
- Mantener instalado un servicio de antivirus en el dispositivo.

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