	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 019	Fecha: 19-01-2022
		Página: 7 de 9

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**			
Nombre de la alerta	Campaña de Smishing por medio de mensajes de texto (SMS) suplantando la identidad del Banco Interbank.			
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 Smishing por medio de mensaje de texto (SMS) enviados a teléfonos móviles que asegura ser la Entidad Bancaria de Interbank, en donde señala lo siguiente: ***"Interbank @Estimado (a) Cliente, Usted tiene un depósito retenido de 1055 soles en línea de su BONO YANAPAY por prevención, Valide Aquí: https://bit.ly/AlertalBK"*** incluido un enlace que redirige a un sitio web que simula ser la Banca Móvil de Interbank, con el objetivo robar datos personales y/o bancarios vinculado a la cuenta de la víctima.

2. Proceso del ataque phishing:

Figura N° 01: Mensaje de texto enviado desde el número de teléfono 971518510, advierte a la víctima, sobre un depósito de dinero retenido para solucionarlo debe validar sus datos ingresando al enlace.

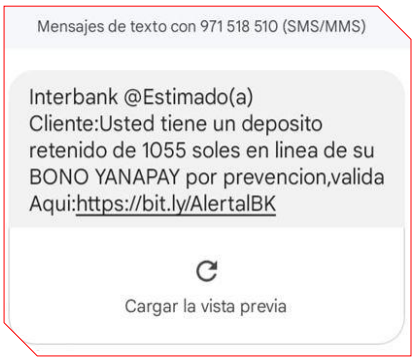


Figura N° 02: Una vez hecho clic en el enlace, es redirigido un sitio que simula ser la Banca móvil de Interbank, en el que visualiza la pantalla una imagen del "Yanapay Perú", que insta a la víctima, aceptar las condiciones para continuar.

Figura N° 03: Sitio web que suplanta la identidad de la Banca Móvil de Interbank, solicita a la víctima, ingresar sus credenciales de acceso (Número de tarjeta, DNI y clave web).

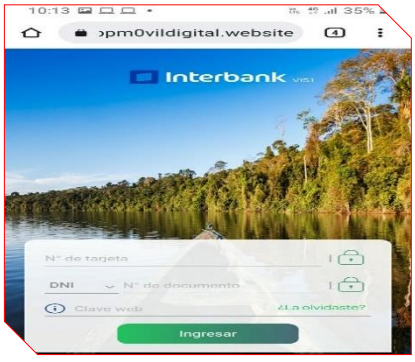


Figura N° 04: Una vez ingresado las credenciales de acceso, se abre una ventana que requiere actualizar los datos, ingresando el número de teléfono y operador móvil se encuentra utilizado.

Figura N° 05: Una vez actualiza los datos, aparece otra venta indicando por seguridad su cuenta se encuentra inhabilitada, para realizar compras activas la tarjeta completando los datos.

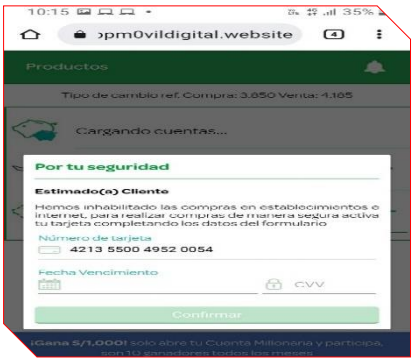
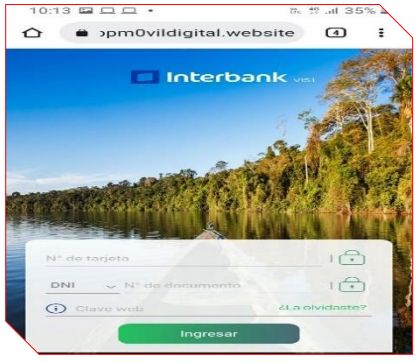
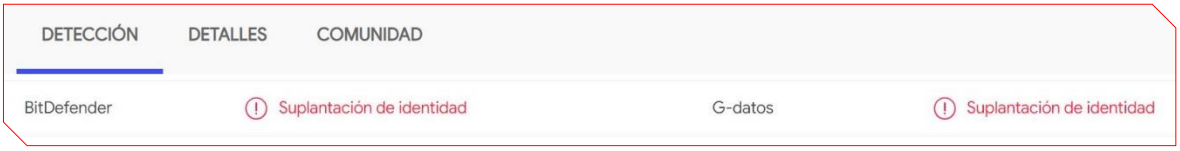


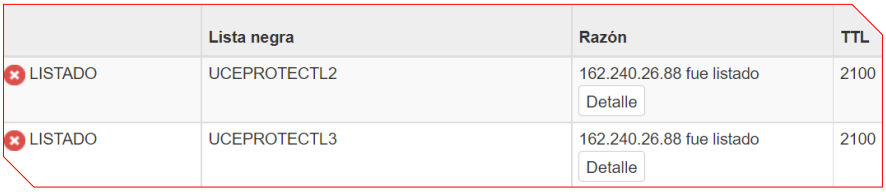
Figura N° 06: Finalmente es redirigido al sitio faso de la Banca Móvil de Interbank, aludiendo un aparente error de autenticación, sin embargo, los datos fueron capturados.



3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultados que, DOS (02) proveedores de seguridad informática alertan como **PHISHING.**
   - URL Final: https[:]//appm0vildigital[.]website/1642602826/inicio/login
   - Dominio: appm0vildigital[.]sitio web
   - Dirección IP: 162[.]240[.]26[.]88
   - Código De Estado: 200
   - Longitud Corporal: 4.59 KB
   - Cuerpo SHA-256: a6b98a72656a5813e8265b57a7dd49458b3fe32e4b7231459ecf6904c2384635



4. Lista negra:
   - Direccion web: Appm0vildigital[.]sitio web



	Lista negra	Razón	TTL
LISTADO	UCEPROTECTL2	162.240.26.88 fue listado Detalle	2100
LISTADO	UCEPROTECTL3	162.240.26.88 fue listado Detalle	2100

5. Cómo funciona el phishing:
   - Se distribuye a través de los correos electrónicos, adjuntando enlaces que redirige a sitios web fraudulentos en los que solicitan información personal.
   - Los ciberdelincuentes utilizan como medios de propagación del phishing: WhatsApp, telegram, redes sociales, SMS entre otros.
   - Los ciberdelincuentes intentan suplantar a una entidad legitima (organismo público, entidad financiera, servicio técnico, etc.).
6. Referencia:
   - Phishing o suplantación de identidad: Método utilizado por los ciberdelincuentes para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.
7. Recomendaciones:
   - Asegurarse que la página a la que intentas ingresar sea el sitio oficial de tu entidad bancaria.
   - Evitar acceder a enlaces que llegan inesperadamente por mensajes texto (SMS).
   - Verificar la dirección del remitente y que coincida que con el servicio al que hace referencia.
   - Evitar guardar información bancaria en el dispositivo móvil.
   - Asegurarse de contar con una solución de seguridad, tanto en dispositivos de escritorio como en móviles, ya que sirven como barrera protectora ante sitios maliciosos.

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