	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 007	Fecha: 07-01-2022
		Página: 7 de 9

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de phishing que se difunde a través de mensajes de texto (SMS) supuestamente proveniente 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 Financiero		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una nueva campaña de phishing que se difunde a través de mensajes de textos (SMS) a teléfono móviles, supuestamente provenientes del Banco Interbank, en el cual anuncia lo siguiente: "Usted ha sido beneficiado por el bono de trabajadores del sector privado, por monto de S/. 210.00, consulte aquí", adjunto un enlace que redirige a una web fraudulenta del Banco Interbank, con el objetivo robar credenciales de acceso, datos personales y bancarios vinculado a la cuenta.
2. Mediante Resolución Ministerial N° 263-2021-TR, el Ministerio de Trabajo y Promoción del Empleo (MTPE), aprobó el listado de trabajadores formales que serían beneficiados con el bono extraordinario de S/210. Esta medida constituye un paso previo hacia la efectivización del cobro que, tal como contempla el Decreto de Urgencia N° 105-2021, favorece al personal formal del sector privado.
3. Proceso del ataque phishing:

Imagen 01: Mensaje de texto (SMS/MM) enviado desde el teléfono +51950452228 insta a los supuestos beneficiarios del Bono Extraordinario de S/. 210, hacer clic en el enlace.

Imagen 02: Una vez hecho clic en el enlace es redirigido a un sitio web falso del Banco Interbank, donde solicita el ingreso de credenciales de acceso (tarjeta, DNI y clave web).

Imagen 03: Pasado unos segundos, es redirigido al sitio web oficial del Banco Interbank, aludiendo un aparente error, sin embargo, los datos fueron capturados.

4. Comparación del sitio web oficial del Banco Interbank con el fraudulento:

SITIO OFICIAL

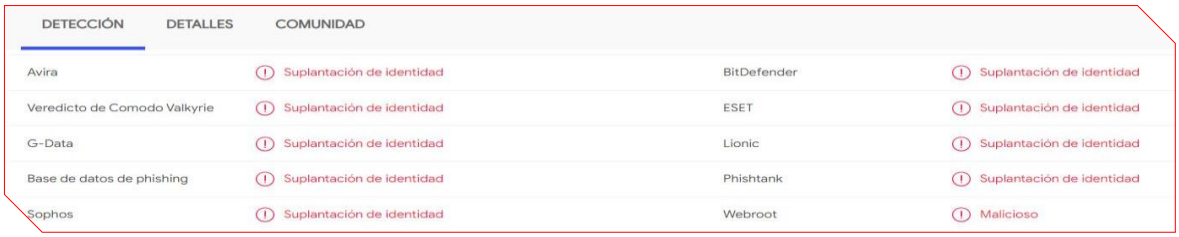
URL: https://bancaporinternet.interbank.pe/login

SITIO FRAUDULENTO

URL: hXXps://www[.]bankaenlinea-interbark[.]com/16414[...]/inicio/login

- Existe similitud entre ambas páginas, en imagen, fondo y escritura la diferencia se encuentra en la URL.
- La URL falsa utiliza protocolo HTTPS, no significa que la web sea segura.
- La URL falsa está mal escrita y los caracteres ambiguos.

5. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultados que, DIEZ (10) proveedores de seguridad informática alertan como **PHISHING.**
   - Análisis de la URL: hXXps[:]//www[.]bankaenlinea-interbark[.]com/16414[...]/inicio/login



   - Indicadores de compromiso:
     - URL Final: hXXps[:]//www[.]bankaenlinea-interbark[.]com/16414[...]/inicio/login
     - Dominio: www[.]bankaenlinea-interbark[.]com
   - Lista negra:
     - Dirección web: Bankaenlinea-interbark[.]com

6. Cómo funciona el phishing:
   - Los ciberdelincuentes a través de los correos electrónicos adjuntan enlaces que redirige a sitios webs 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.).

7. Referencia:
   - Phishing o suplantación de identidad: Es una técnica fraudulenta consiste en engañar al usuario solicitando información personal, contraseñas, datos bancarios etc., a través del correo electrónico o redirigiendo a la víctima a una copia falsa de una página web donde se le solicita el ingreso de los datos que se quieren obtener.

8. Recomendaciones:
   - No responder a los mensajes fraudulentos enviado desde teléfono móviles que incluyan enlaces.
   - No guardar información bancaria en el dispositivo móvil.
   - Ante la duda, no responder a los SMS.
   - Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
   - Visualizar los sitios web que se ingresen sean los oficiales.

Fuentes de información	Análisis propio de redes sociales y fuente abierta