	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°298	Fecha: 15-12-2023
		Página: 7 de 9

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Campaña de Smishing o mensaje de texto falso (SMS) que suplanta la identidad del Banco de la Nación		
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 Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. **ANTECEDENTES:**

Se identificó, a través de la vigilancia y seguimiento de amenazas en el ciberespacio, una nueva campaña de Smishing o mensajes de texto falso (SMS), realizada por ciberdelincuentes. Esta campaña suplanta la identidad del banco de la Nación, con el fin de obtener credenciales de acceso, así como información personal y bancaria de los usuarios.

2. **DETALLES:**

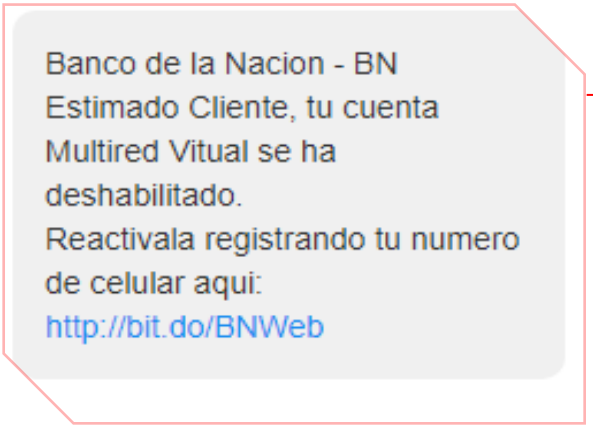


Imagen 1: Mensaje de texto falso (SMS) enviado supuestamente por el banco de la Nación, incita a la víctima hacer clic en el enlace adjunto.

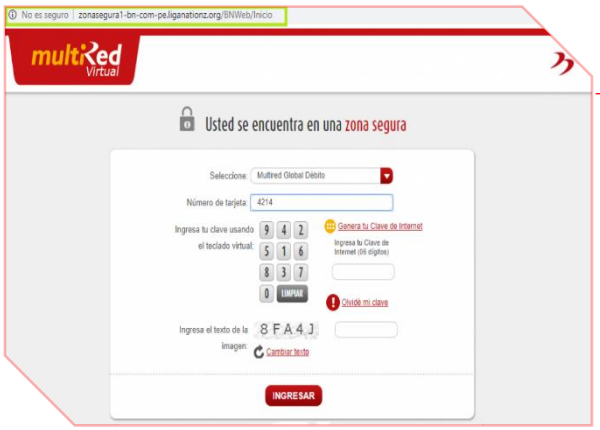
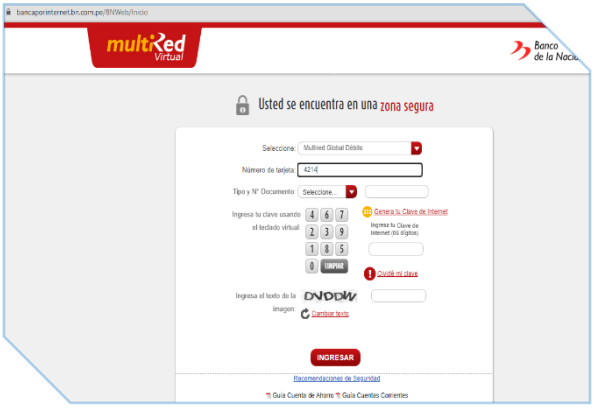


Imagen 2: Después de haber hecho clic, en el enlace, es redirigido al sitio web falso del banco de la Nación, solicitando ingresar las credenciales de acceso tales como el número de tarjeta y clave de internet (06 dígitos).

Imagen 3: Una vez ingresada las credenciales de acceso, es redirigido al sitio web oficial del banco de la Nación, aludiendo un aparente error de autenticación; sin embargo, los datos ingresados fueron capturados, por los ciberdelincuentes.

A. Comparación entre el sitio web oficial del banco de la Nación y el sitio web falso para identificar diferencias y similitudes:

SITIO WEB OFICIAL	SITIO WEB FRAUDULENTO
hxxps://bancaporinternet.bn.com.pe/BNWeb/Inicio	hxxps(:)//zonasegura1(-)bn(-)com(-)pe(.)liganationz(.)org/BNWeb/inicio



- Los dos sitios web tienen una apariencia y estructura similar.
- La diferencia principal radica en el dominio, ya que el sitio fraudulento no concuerda con la dirección oficial del BN.
- Ambos sitios cuentan con el protocolo seguro de transferencia de hipertexto (HTTPS), lo que puede convencer aún más a las víctimas al acceder al sitio falso del banco de la Nación.

B. Los proveedores de seguridad informática emiten una alerta sobre el riesgo de suplantación de identidad mediante técnicas de phishing:

Avira	Suplantación de identidad	BitDefender	Suplantación de identidad
Clúster25	Suplantación de identidad	Emsisoft	Suplantación de identidad
Fortinet	Suplantación de identidad	Datos G	Suplantación de identidad
Kaspersky	Suplantación de identidad	Ieonico	Malicioso
Netcraft	Malicioso	Sofos	Suplantación de identidad

C. Indicadores de compromiso (IoC)

- URL : hxxps(:)//zonasegura1(-)bn(-)com(-)pe(.)liganationz(.)org/BNWeb/inicio
- Dominio : zonasegura1(-)bn(-)com(-)pe(.)liganationz(.)org

D. Referencia:

- El Smishing es una técnica que consiste en el envío de un SMS por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima red social, banco, institución pública, etc. con el objetivo de robarle información privada o realizarle un cargo económico. Generalmente el mensaje invita a llamar a un número de tarificación especial o acceder a un enlace de una web falsa bajo un pretexto.

3. RECOMENDACIONES:

- Verificar minuciosamente la URL para asegurarse de que corresponda al sitio web oficial.
- Tener en cuenta que las instituciones bancarias no solicitan la actualización de datos confidenciales en línea.
- Ingresar datos confidenciales solo desde fuentes oficiales.
- Evitar seguir instrucciones de sitios web sospechosos o de reputación dudosa.
- Mantener el antivirus actualizado sirve como primera línea de defensa contra ataques cibernéticos.
- Abstenerse de compartir la URL con amigos o familiares para evitar riesgos.

Fuente de Información:	Análisis propio de redes sociales y fuente abierta.