	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°309		Fecha: 29-12-2023
			Página: 8 de 10
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Suplantación de entidad del Banco de la Nación, con la finalidad de propagar Malware "Adware", a través de mensajería instantánea WhatsApp		
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:

A través de las acciones propias de la especialidad en el ciberespacio, se ha detectado una nueva campaña de propagación del Malware denominado "Adware o software malicioso", a través de mensajes fraudulentos de WhatsApp, simulando ser la entidad del Banco de la Nación, temática **"Participa en el evento de Año Nuevo del Banco de la Nación y gana un iPhone 15"**, en la que se adjunta un enlace (URL) que redirige a un sitio web falso del Banco de la Nación, con el objetivo infectar los dispositivos de los víctimas, con publicidad no deseada o engañosa proveniente de páginas web.

2. DETALLES:

Imagen 1: Mensaje que llega a través de WhatsApp y que da inicio al engaño



Imagen 2: Encuesta que debe completar la víctima, como parte del proceso de 1 al 4

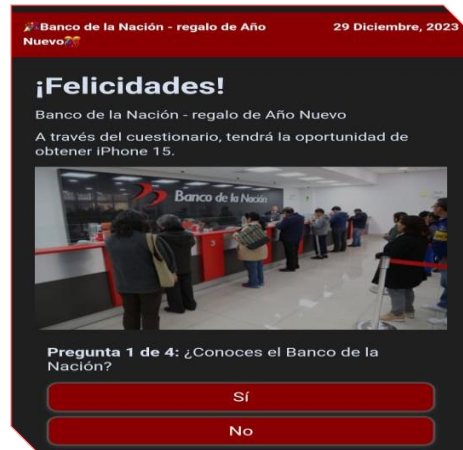


Imagen 3: Para obtener el premio invita a la víctima, a participar de un juego



Imagen 4: La victima siempre gana el premio y luego se solicita compartir esta información



Imagen 5: Instan en la que se debe compartir el engaño con los contactos de WhatsApp

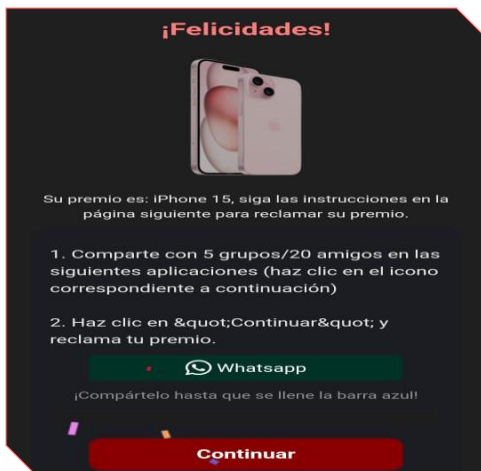
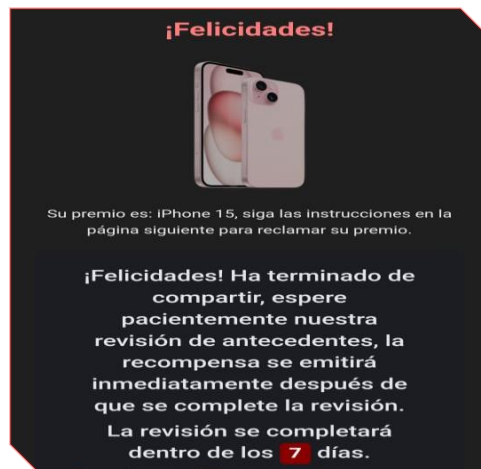


Imagen 6: Paso final se prometió el iPhone 15 por una semana, pero el dispositivo resultó infectado por Adware.



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



B. Indicadores de compromiso (IoC)

- URL : hXXps[:]//enrollmentpeninsula[.]top/oioTTTBmpw?vawn1703860544589
- Dominio : inscripciónpeninsula[.]arriba
- IP : 104[.]21[.]21[.]234
- Código : 200
- Longitud : 1,18 KB
- SHA-256 : 4e5830e39d040c0b539729bd0d4d1c0dc06721d5abb7c61412488f3c244d3cfb

C. Referencia:

- Adware es un software o programa que muestra algún tipo de publicidad no deseada o engañosa desde página webs o con la instalación de algún programa. Su objetivo es obtener algún beneficio económico o incluso almacenar información privada.

3. RECOMENDACIONES:

- Actualizar regularmente el sistema operativo, navegadores y programas con las últimas versiones y parches de seguridad.
- Evitar hacer clic en enlaces sospechosos o descargar archivos de origen desconocido o no confiable.
- Respalda tus archivos importantes en un lugar seguro puede ayudar a recuperar información en caso de una infección.
- Obtener software solo de fuentes confiables, como sitios web oficiales y tiendas de aplicaciones reconocidas.
- Desconfiar de Regalos, obsequios o premios que llegan a través de las plataformas digitales.

Fuente de Información:

Análisis propio de redes sociales y fuente abierta.