Nro. Alerta:	EC-2025-046	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	26-ago-2025	**Campaña de información de Suplantación de Identidad a Operadoras del Servicio Móvil Avanzado en Ecuador**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Fraude – Smishing

Tipo de incidente: Suplantación de identidad y falsificación de archivos.

Nivel de riesgo: Alto

II. INTRODUCCIÓN

El Phishing a través de SMS, conocido como Smishing, es un ciberataque donde los delincuentes envían mensajes de texto engañosos para que las víctimas divulguen información personal o financiera. Estos mensajes a menudo se hacen pasar por entidades legítimas como bancos, operadoras del servicio móvil avanzado o tiendas, creando un sentido de urgencia para que el usuario haga clic en enlaces maliciosos y descargar archivos adjuntos que contienen malware.

El malware, o "software malicioso", es cualquier programa informático diseñado para infiltrarse en un sistema, dañar dispositivos o redes, o robar datos sin el consentimiento del usuario. Se trata de una categoría amplia que incluye virus, gusanos, ransomware, spyware y troyanos, y los ciberdelincuentes lo usan para obtener acceso no autorizado, robar información valiosa como credenciales bancarias, extorsionar a las víctimas o interrumpir servicios esenciales

III. VECTOR DE ATAQUE:

A través de SMS los atacantes usaron el nombre de la Corporación Nacional de Telecomunicaciones CNT y de OTECEL S.A (Movistar) con el objetivo de solicitar a la ciudadanía descargar una aplicación para el supuesto uso de tecnología 5G.

Estas aplicaciones .apk nombradas CNT 5G.apk o 5G_en_en.apk implica varios riesgos de seguridad y privacidad, porque se trata de fuentes no verificadas que contienen código malicioso (malware).

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código postal: 170513 / Quito - Ecuador
Teléfono: +593-2 2946 400
www.arcotel.gob.ec

Nro. Alerta:	EC-2025-046	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	26-ago-2025	**Campaña de información de Suplantación de Identidad a Operadoras del Servicio Móvil Avanzado en Ecuador**	V 1.1

Los archivos .apk pueden contener troyanos, spyware, ransomware o keylogeers que se instalan junto con la App; estos pueden robar contraseñas, interceptar mensajes, encender el micrófono/cámara, o cifrar archivos para pedir rescate. Al instalar, la App puede solicitar permisos excesivos (contactos, ubicación, micrófono, SMS, llamadas); esto expone datos sensibles como fotos, números de cuentas, contraseñas y conversaciones. Un .apk modificado puede instalar código oculto que concierta el dispositivo en parte de una botnet o lo use para ataques DDoS. El archivo .apk al no estar verificada por la tienda, puede no funcionar bien en su verión de Android, generar errores, bloqueos o consumo excesivo de batería y datos.

IV. INDICADORES DE COMPROMISO:

- **SMS con el siguiente texto:**

  “Bienvenido a CNT ¿Estás listo para disfrutar de la mejor red 5g de Ecuador?, solo descarga la aplicación 5G de CNT y disfruta de sus velocidades.”

  “Bienvenido a MOVISTAR ¿Estás listo para disfrutar de la mejor red 5g de ECUADOR?, solo descarga la aplicación 5G de movistar y disfruta de sus velocidades.”

- ***Archivo ejecutable (.apk) denominado:***

  1. *CNT 5G.apk*
  2. *5G_en_en.apk*

- ***Número de telefónico celular:***

  1. *098 493 2771.*

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código postal: 170513 / Quito - Ecuador
Teléfono: +593-2 2946 400
www.arcotel.gob.ec

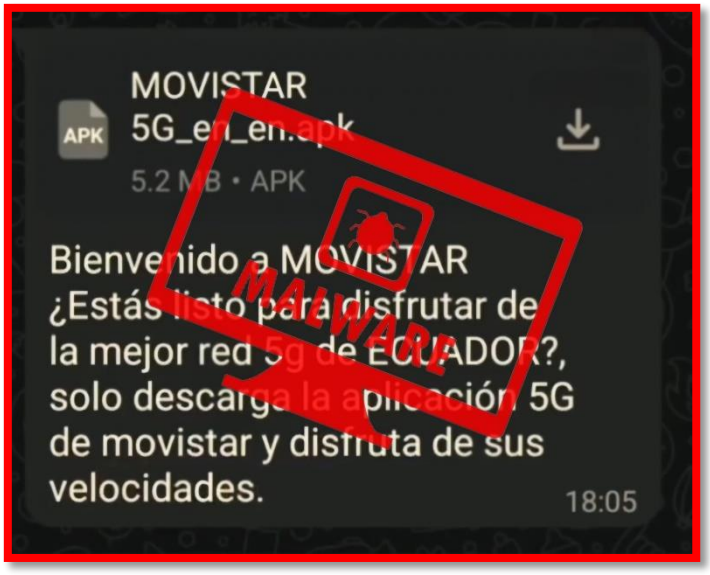
Nro. Alerta:	EC-2025-046	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	26-ago-2025	**Campaña de información de Suplantación de Identidad a Operadoras del Servicio Móvil Avanzado en Ecuador**	V 1.1

V. IMÁGENES DE LA CAMPAÑA DE SMISHING.

Gráfica 1.- SMS que suplanta a CNT ofreciendo servicios 5G mediante App maliciosa.

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código postal: 170513 / Quito - Ecuador
Teléfono: +593-2 2946 400
www.arcotel.gob.ec

Nro. Alerta:	EC-2025-046	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	26-ago-2025	**Campaña de información de Suplantación de Identidad a Operadoras del Servicio Móvil Avanzado en Ecuador**	V 1.1



Gráfica 2.- SMS que suplanta a MOVISTAR ofreciendo servicios 5G mediante App maliciosa.

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Instalar y mantener actualizado una solución Antivirus en su dispositivo.
- No descargar archivos apk. con lo que se ofrece conectar a redes 5G, indicados en la sección indicadores de compromisos
- Si es necesario instalar archivos .apk en su dispositivo descargarlo sólo de fuentes confiables como Google Play Store, AppGallery, Galaxy Store u otras tiendas oficiales.
- Verificar permisos antes de instalar.
- Mantener el sistema operativo de su dispositivo móvil actualizado.
- No habilitar “instalación de orígenes desconocidos” salvo casos muy puntuales y de confianza.
- Mantenerse informado continuamente sobre tipos de amenazas en el internet.

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código postal: 170513 / Quito - Ecuador
Teléfono: +593-2 2946 400
www.arcotel.gob.ec

Nro. Alerta:	EC-2025-046	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	26-ago-2025	**Campaña de información de Suplantación de Identidad a Operadoras del Servicio Móvil Avanzado en Ecuador**	V 1.1

- Validar si los sitios web en los que se navega son seguros (se utiliza el puerto https) y oficiales (el dominio corresponde al nombre de la empresa, no tiene errores ortográficos).
- Hacer caso omiso a correos, links o mensajes de dudosa procedencia y márcalos como spam o bloquearlos y comunicar a su departamento técnico.
- Ante cualquier duda contactarse directamente con la persona o empresa suplantada para su comprobación y/o denuncia.
- En caso de haber ingresado los datos personales en el sitio web fraudulento, cambiar la contraseña de las cuentas y comunicarse inmediatamente con la empresa suplantada para la toma de acciones de remediación.
- Nunca entregue los usuarios y contraseñas solicitados a través de correos electrónicos, redes sociales o llamadas telefónicas.

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código postal: 170513 / Quito - Ecuador
Teléfono: +593-2 2946 400
www.arcotel.gob.ec