Nro. Alerta:	AL-2025-061	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		
Fecha:	04-dic-2025	**Suplantación de Identidad "Servicio de Rentas Internas - SRI"**	V 1.1

I. DATOS GENERALES:

Clase de alerta: App Fraud

Tipo de incidente: Falsificación de registros o identidad.

Nivel de riesgo: Alto

II. INTRODUCCIÓN

El fraude a través de aplicaciones móviles es una modalidad delictiva en la que los atacantes distribuyen aplicaciones aparentemente legítimas, pero que contienen código malicioso diseñado para comprometer la seguridad del usuario. Estas aplicaciones suelen ser promovidas mediante técnicas de ingeniería social, mensajes engañosos o enlaces fraudulentos, con el fin de inducir a la víctima a instalarlas en su dispositivo.

Una vez instalada, la aplicación maliciosa puede obtener permisos indebidos, capturar información sensible, interceptar comunicaciones (incluidos SMS y códigos de autenticación), acceder a credenciales bancarias o incluso tomar control remoto del dispositivo. El objetivo principal de este tipo de fraude es el robo de datos personales, credenciales de acceso o recursos financieros de la víctima.

Este tipo de ataques representa un riesgo significativo para la seguridad digital, por lo que se recomienda a los usuarios instalar aplicaciones únicamente desde tiendas oficiales, verificar los permisos solicitados, y desconfiar de enlaces recibidos por canales no verificados.

III. VECTOR DE ATAQUE:

El vector de ataque se inicia cuando la víctima accede a una página web falsa que suplanta a un portal institucional legítimo. Desde este sitio fraudulento, el usuario es inducido a descargar una aplicación móvil alojada en un servidor no reconocido y fuera de los canales oficiales de distribución.

Una vez instalada la aplicación, el sistema simula un proceso de registro legítimo, solicitando inicialmente el número de teléfono y la creación de una clave de acceso. Acto seguido, la aplicación exige el registro de una contraseña de consulta de

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

cuatro dígitos y una contraseña adicional de transacción de seis dígitos, capturando así información crítica que posteriormente puede ser utilizada para actividades ilícitas.

En etapas posteriores, la aplicación solicita al usuario habilitar permisos de "Accesibilidad" y el permiso de "Teléfono móvil para transmitir contenido" para el supuesto funcionamiento del aplicativo "SRI Móvil". Para activar estos permisos, el usuario debe acceder a la configuración del dispositivo y otorgar "ajustes restringidos", proceso que requiere la autenticación mediante PIN, patrón, huella dactilar o contraseña del teléfono. Al aprobar estos permisos, la aplicación obtiene control total sobre el dispositivo comprometido.

Posteriormente, la aplicación inicia un proceso de sincronización con el teléfono, durante el cual solicita nuevamente la huella dactilar y el reconocimiento facial. Esta acción tiene como finalidad capturar y almacenar información biométrica de la víctima. Con el control del dispositivo, las credenciales recopiladas y los datos biométricos, los atacantes pueden ejecutar transacciones bancarias, solicitar préstamos, realizar avances de tarjetas y llevar a cabo diversas actividades ilícitas sin el conocimiento ni intervención del usuario.

IV. INDICADORES DE COMPROMISO:

El indicador de compromiso reportado y asociado a la campaña maliciosa son los enlaces que dirigen a los sitios web fraudulentos:

- ***Sitios web:***

  https://sriimpuestos-ec.com/

- ***Ip´s:***

  172.67.214.231 (*fuente virustotal.com*)

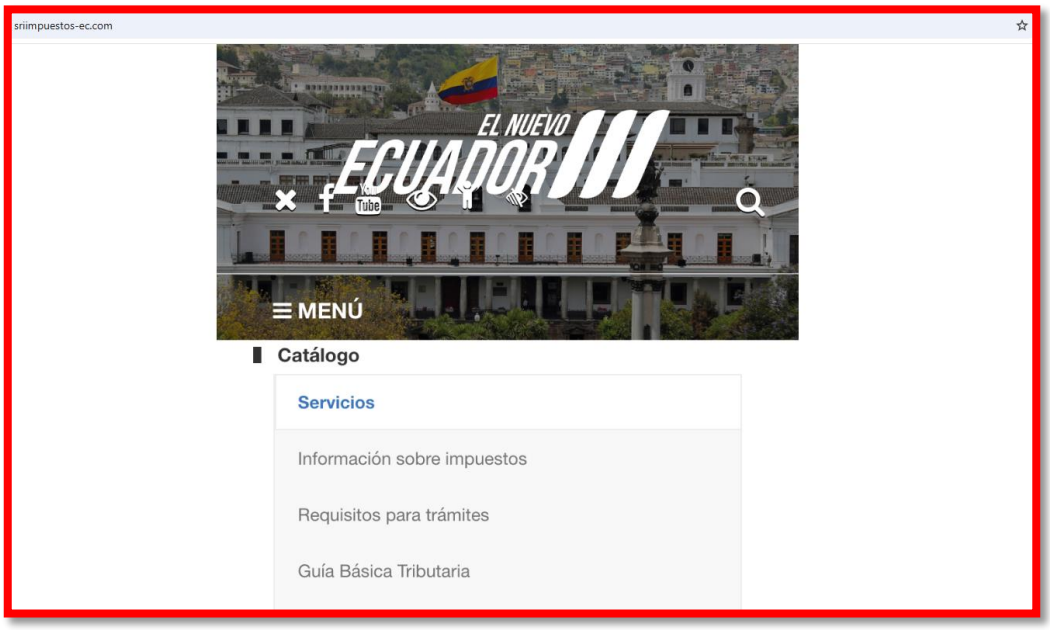
- ***Aplicativo:***

  SRI Móvil.apk

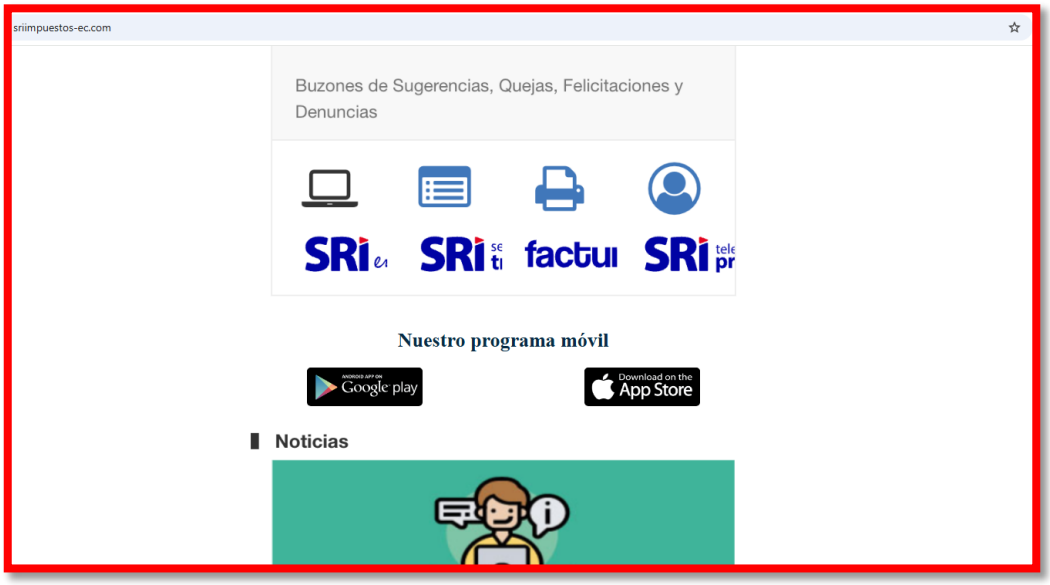
Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Nro. Alerta:	AL-2025-061	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		
Fecha:	04-dic-2025	**Suplantación de Identidad "Servicio de Rentas Internas - SRI"**	V 1.1

V. IMÁGENES DE LA CAMPAÑA DE SUPLANTACIÓN DE IDENTIDAD.



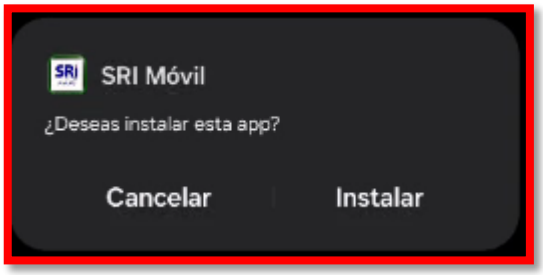
Gráfica 1.- Sitio web que suplanta a la Servicio de Rentas Internas.



Gráfica 2.- Sitio web que suplanta a la Servicio de Rentas Internas, utilizado como punto de descarga del aplicativo malicioso.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Nro. Alerta:	AL-2025-061	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		
Fecha:	04-dic-2025	**Suplantación de Identidad "Servicio de Rentas Internas - SRI"**	V 1.1



Gráfica 3.- Aplicativo descargado del sitio web fraudulento.

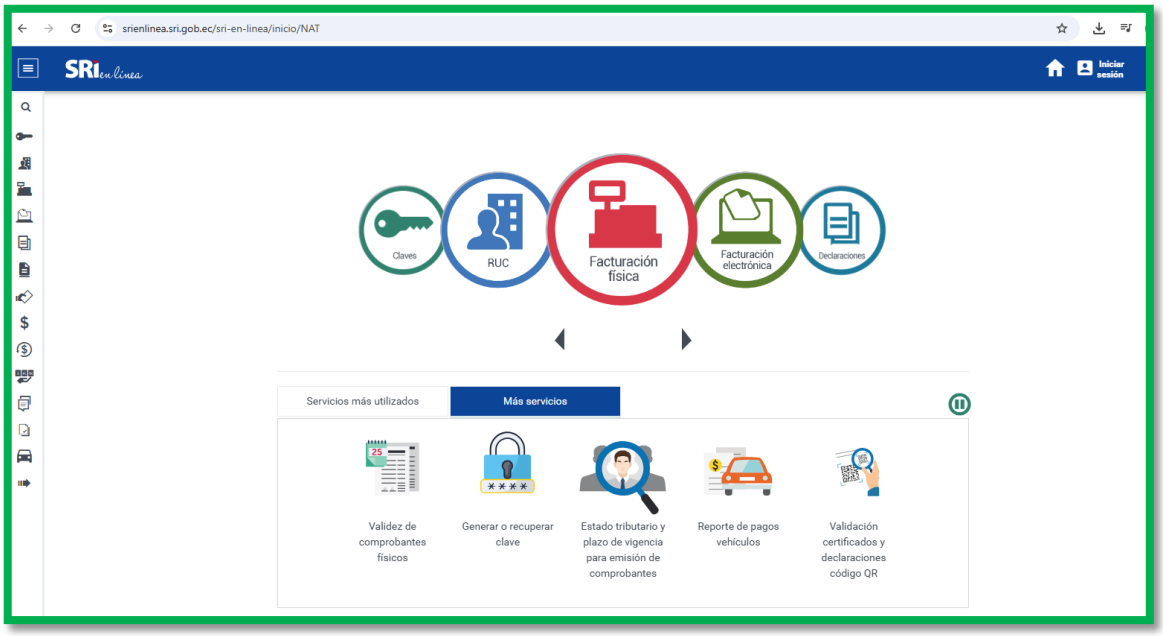
Gráfica 4.- Página de inicio del aplicativo fraudulento.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Nro. Alerta:	AL-2025-061	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		
Fecha:	04-dic-2025	**Suplantación de Identidad "Servicio de Rentas Internas - SRI"**	V 1.1

VI. SITIO WEB REAL DEL SERVICO DE RENTAS INTERNAS

https://srienlinea.sri.gob.ec/



Gráfica 2.- Información en Página WEB real del Registro Civil

VII. RECOMENDACIONES:

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

- 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.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Nro. Alerta:	AL-2025-061	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		
Fecha:	04-dic-2025	**Suplantación de Identidad "Servicio de Rentas Internas - SRI"**	V 1.1

- 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.
- Instalar y mantener actualizado una solución Antivirus.
- Bloquear los sitios web o direcciones de correo electrónicos indicados en la sección indicadores de compromisos.
- Mantenerse informado continuamente sobre tipos de amenazas en el internet.
- Instalar archivos .apk en su dispositivo descargarlo sólo de fuentes confiables como Google Play Store, AppGallery, Galaxy Store u otras tiendas oficiales.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec