Nro. Alerta:	EC-2023-01	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	19-ene-2023	**EcuCERT advierte nueva campaña de suplantación de identidad "SRI"**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Fraude – Scam

Tipo de incidente: Falsificación de registros o identidad.

Nivel de riesgo: Alto

II. INTRODUCCIÓN

El email spoofing, o correo de suplantación de identidad, es una técnica empleada en los ataques de spam y de phishing para hacerle pensar a un usuario que un mensaje proviene de una persona o entidad que conocen o en la que confían. En los ataques de spoofing, el remitente falsifica los encabezados del correo electrónico para que el software cliente muestre la dirección de remitente fraudulenta, que la mayoría de los usuarios acepta tal como la ven. A menos que inspeccionen cuidadosamente el encabezado, los usuarios solamente verán el remitente falso en el mensaje..

III. VECTOR DE ATAQUE:

A través de correo electrónico circula una campaña maliciosa que invita al usuario a ingresar a un supuesto enlace que descarga un archivo malicioso.

IV. INDICADORES DE COMPROMISO:

El indicador de compromiso reportado y asociado a la campaña maliciosa es la cuenta de correo camiloandres0824@outlook.com.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2023-01	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	19-ene-2023	**EcuCERT advierte nueva campaña de suplantación de identidad "SRI"**	V 1.1

V. IMAGEN DE LA CAMPAÑA

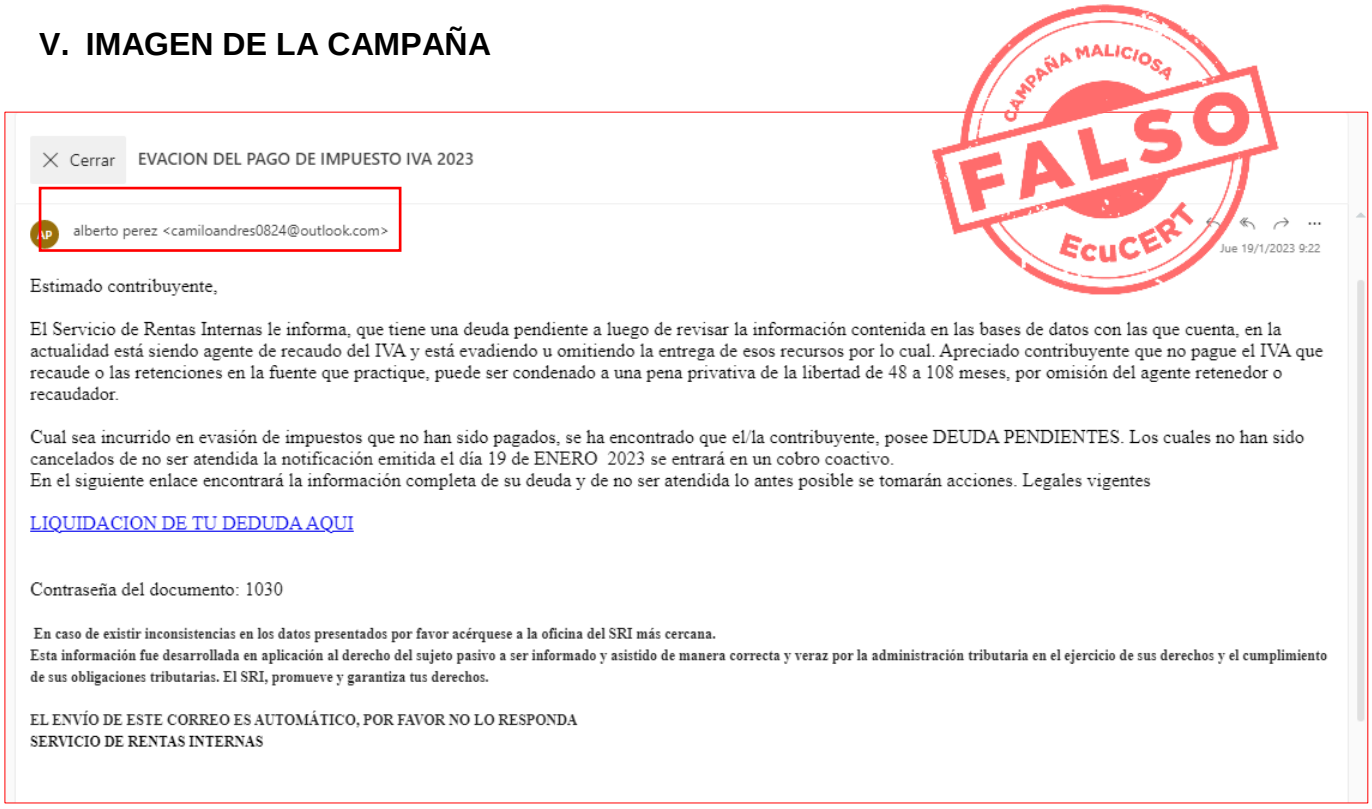

Figura 1.- ***Campaña maliciosa a nombre del SRI***

VI. 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).

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2023-01	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	19-ene-2023	**EcuCERT advierte nueva campaña de suplantación de identidad "SRI"**	V 1.1

- 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.
- Instalar y mantener actualizado una solución Antivirus.
- Bloquear los sitios web o direcciones de correo electrónicos indicados en la sección indicadores de compromisos.
- Informarse continuamente sobre tipos de amenazas en el internet.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec