

Nro. Alerta:	EC-2023-01	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
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.

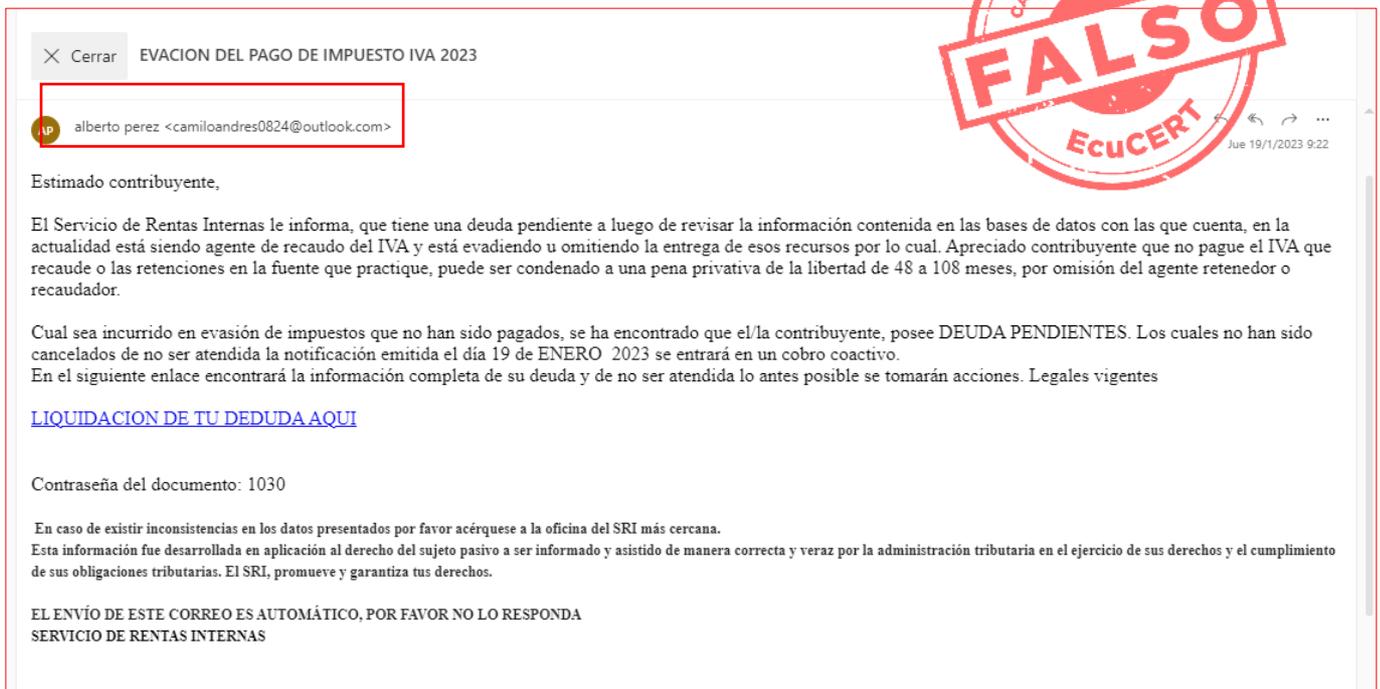
IV. INDICADORES DE COMPROMISO:

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



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

V. IMAGEN DE LA CAMPAÑA



The image shows a screenshot of an email titled "EVACION DEL PAGO DE IMPUESTO IVA 2023" from "alberto perez <camiloandres0824@outlook.com>". The email body contains a warning about tax evasion and a link to "LIQUIDACION DE TU DEDUDA AQUI". A large red stamp with the word "FALSO" and "EcuCERT" is overlaid on the right side of the screenshot. The email text includes: "Estimado contribuyente, El Servicio de Rentas Internas le informa, que tiene una deuda pendiente a luego de revisar la información contenida en las bases de datos con las que cuenta, en la actualidad está siendo agente de recaudo del IVA y está evadiendo u omitiendo la entrega de esos recursos por lo cual. Apreciado contribuyente que no pague el IVA que recaude o las retenciones en la fuente que practique, puede ser condenado a una pena privativa de la libertad de 48 a 108 meses, por omisión del agente retenedor o recaudador. Cual sea incurrido en evasión de impuestos que no han sido pagados, se ha encontrado que el/la contribuyente, posee DEUDA PENDIENTES. Los cuales no han sido cancelados de no ser atendida la notificación emitida el día 19 de ENERO 2023 se entrará en un cobro coactivo. En el siguiente enlace encontrará la información completa de su deuda y de no ser atendida lo antes posible se tomarán acciones. Legales vigentes LIQUIDACION DE TU DEDUDA AQUI Contraseña del documento: 1030 En caso de existir inconsistencias en los datos presentados por favor acérquese a la oficina del SRI más cercana. Esta información fue desarrollada en aplicación al derecho del sujeto pasivo a ser informado y asistido de manera correcta y veraz por la administración tributaria en el ejercicio de sus derechos y el cumplimiento de sus obligaciones tributarias. El SRI, promueve y garantiza tus derechos. EL ENVÍO DE ESTE CORREO ES AUTOMÁTICO, POR FAVOR NO LO RESPONDA SERVICIO DE RENTAS INTERNAS".

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).

Nro. Alerta:	EC-2023-01	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
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.

