Nro. Alerta:	EC-2022-24	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	25-feb-2022	**EcuCERT advierte nueva campaña de suplantación de identidad "Función Judicial"**	V 1.0

I. DATOS GENERALES:

Clase de alerta: Fraude – Scam

Tipo de incidente: Phishing

Nivel de riesgo: Alto

II. INTRODUCCIÓN

La técnica de Phishing es un método de fraude a través de medios digitales que pretende engañar a las víctimas para obtener información personal confidencial tales como credenciales de cuentas de correo, banca electrónica, etc.

III. VECTOR DE ATAQUE:

A través de correos electrónicos se remite una supuesta notificación de proceso judicial por parte de la "*UNIDAD JUDICIAL*":

Correo 1:
El correo incita al usuario a descargar un archivo con el nombre "Citación de la Fiscalía General.pdf". El archivo adjunto supuestamente contiene información del proceso.

Correo 2:
El correo incita al usuario a hacer clic en un link para la descarga de documentos del supuesto proceso judicial; al hacer clic en el link re direcciona a un sitio web malicioso para el ingreso de datos personales por parte de la víctima.

IV. INDICADORES DE COMPROMISO:

Los indicadores de compromiso reportados y asociados a la campaña maliciosa son:

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-2022-24	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	25-feb-2022	**EcuCERT advierte nueva campaña de suplantación de identidad "Función Judicial"**	V 1.0

Remitentes de los correos electrónicos maliciosos:

- hugoluna29@hotmail[.]com
- FISCALIA-GOV@hotmail[.]com

V. IMAGEN DE LA CAMPAÑA

Correo con archivo adjunto

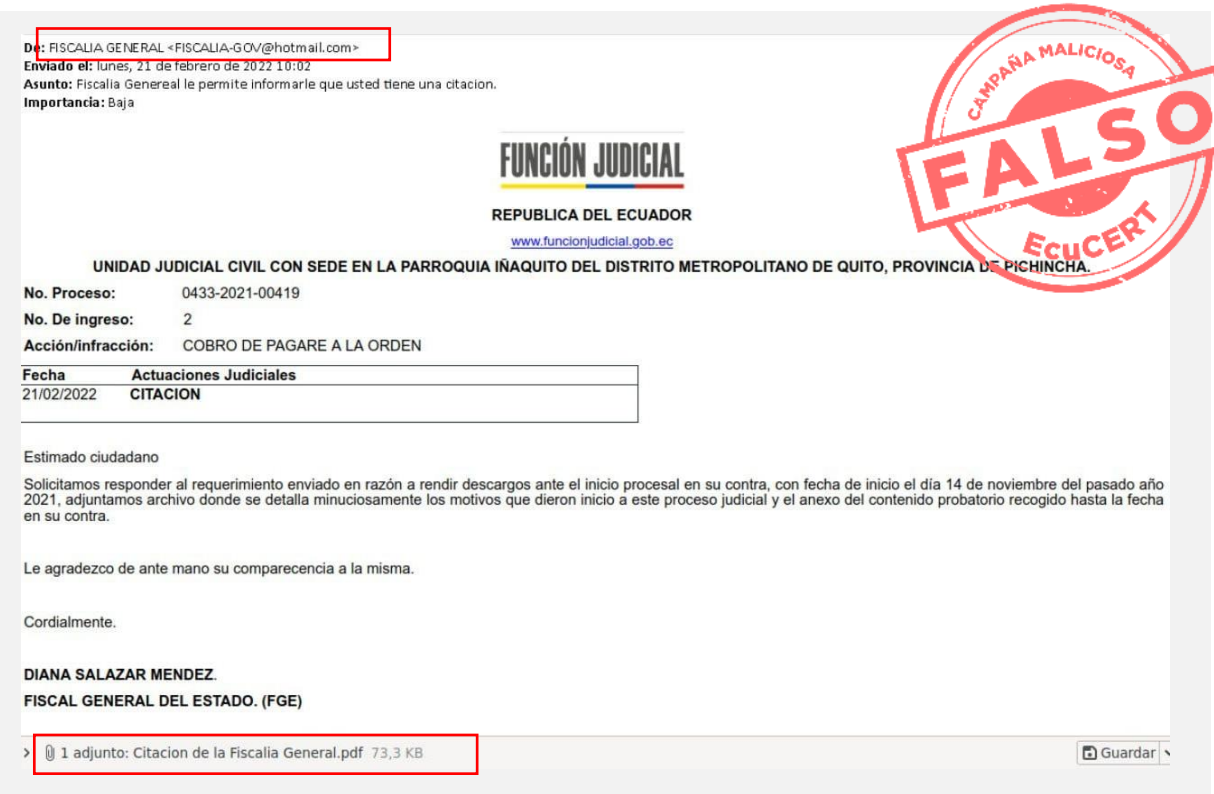

Figura 1.- ***Campaña maliciosa a nombre de Función Judicial con adjunto***

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-2022-24	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	25-feb-2022	**EcuCERT advierte nueva campaña de suplantación de identidad "Función Judicial"**	V 1.0

Correo con link para descarga

Figura 2.- ***Campaña maliciosa a nombre de Función Judicial con link***

VI. RECOMENDACIONES:

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

- Hacer caso omiso a correos, links o mensajes de dudosa procedencia y márcalos como spam para bloquearlos.

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-2022-24	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	25-feb-2022	**EcuCERT advierte nueva campaña de suplantación de identidad "Función Judicial"**	V 1.0

- 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).
- Ante cualquier duda contactarse directamente con la persona o empresa suplantada para su comprobación y/o denuncia.
- Nunca entregue los usuarios y contraseñas solicitados a través de correos electrónicos, redes sociales o llamadas telefónicas, sitios web desconocidos, etc.
- 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.
- Instalar y mantener actualizado una solución antivirus / antimalware.
- Bloquear el URL y la dirección de correo indicada en la sección indicadores de compromisos.
- Informarse continuamente sobre tipos de amenazas en la internet.

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