

Nro. Alerta:	EC-2022-24	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
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 se 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:



Nro. Alerta:	EC-2022-24	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
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



De: FISCALIA GENERAL <FISCALIA-GOV@hotmail.com>
Enviado el: lunes, 21 de febrero de 2022 10:02
Asunto: Fiscalía General le permite informarle que usted tiene una citación.
Importancia: Baja

FUNCION JUDICIAL
 REPUBLICA DEL ECUADOR
www.funcionjudicial.gob.ec

UNIDAD JUDICIAL CIVIL CON SEDE EN LA PARROQUIA IÑAQUITO DEL DISTRITO METROPOLITANO DE QUITO, PROVINCIA DE PICHINCHA.

No. Proceso: 0433-2021-00419
No. De ingreso: 2
Acción/Infracción: COBRO DE PAGARE A LA ORDEN

Fecha	Actuaciones Judiciales
21/02/2022	CITACION

Estimado ciudadano

Solicitamos responder al requerimiento enviado en razón a rendir descargos ante el inicio procesal en su contra, con fecha de inicio el día 14 de noviembre del pasado año 2021, adjuntamos archivo donde se detalla minuciosamente los motivos que dieron inicio a este proceso judicial y el anexo del contenido probatorio recogido hasta la fecha en su contra.

Le agradezco de ante mano su comparecencia a la misma.

Cordialmente.

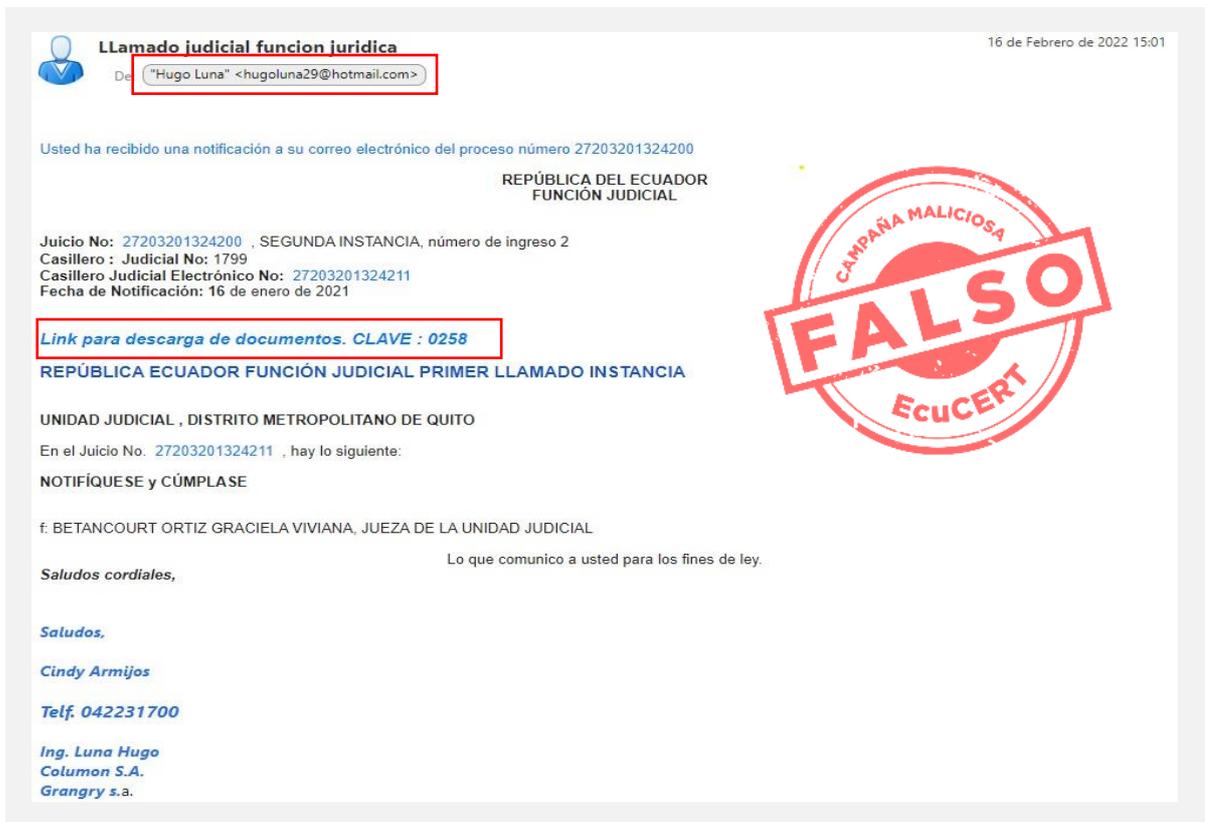
DIANA SALAZAR MENDEZ.
 FISCAL GENERAL DEL ESTADO. (FGE)

>  1 adjunto: Citación de la Fiscalía General.pdf 73,3 KB Guardar

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

Nro. Alerta:	EC-2022-24	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
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



Llamado judicial funcion juridica 16 de Febrero de 2022 15:01

De: "Hugo Luna" <hugoluna29@hotmail.com>

Usted ha recibido una notificación a su correo electrónico del proceso número 27203201324200

REPÚBLICA DEL ECUADOR
FUNCIÓN JUDICIAL

Juicio No: 27203201324200 , SEGUNDA INSTANCIA, número de ingreso 2
Casillero : Judicial No: 1799
Casillero Judicial Electrónico No: 27203201324211
Fecha de Notificación: 16 de enero de 2021

Link para descarga de documentos. CLAVE : 0258

REPÚBLICA ECUADOR FUNCIÓN JUDICIAL PRIMER LLAMADO INSTANCIA

UNIDAD JUDICIAL , DISTRITO METROPOLITANO DE QUITO

En el Juicio No. 27203201324211 , hay lo siguiente:

NOTIFÍQUESE y CÚMPLASE

f. BETANCOURT ORTIZ GRACIELA VIVIANA, JUEZA DE LA UNIDAD JUDICIAL

Lo que comunico a usted para los fines de ley.

Saludos cordiales,

Saludos,

Cindy Armijos

Telf. 042231700

Ing. Luna Hugo
Columon S.A.
Grangry s.a.

FALSO
CAMPAÑA MALICIOSA
EcuCERT

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.



Nro. Alerta:	EC-2022-24	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
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.

