Nro. Alerta:	EC-2022-18	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	04-mar-2022	**EcuCERT advierte nueva campaña de phishing "Función Judicial DMQ"**	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 correo electrónico se remite una supuesta "CITACIÓN FUNCION JUDICIAL PENAL xxxxxx", emitida por la *"UNIDAD JUDICIAL, DISTRITO METROPOLITANO DE QUITO"*; para descargar dicho comprobante, se debe hacer clic en "**Descargue su documento aquí",** el cuál 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:

- Remitente del correo electrónico malicioso: funciondejusticia@ecuador[.]com
- IOC archivo adjunto:
  sha256: ebbc37e280f15408a2ff17bec1151cc64d151e20c1e59209a76b9eb3944d6704
  sha1: 606fb46526b2c6187b00a94b2adb288171797127
  md5: 216e41dd8889798a65852249394a62ad

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-2022-18	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	04-mar-2022	**EcuCERT advierte nueva campaña de phishing "Función Judicial DMQ"**	V 1.0

- DNS:

Dominio: dns.msftncsi.com

- Direcciones IP:

20[.]42[.]65[.]92
31[.]42[.]177[.]191

V. IMAGEN DE LA CAMPAÑA

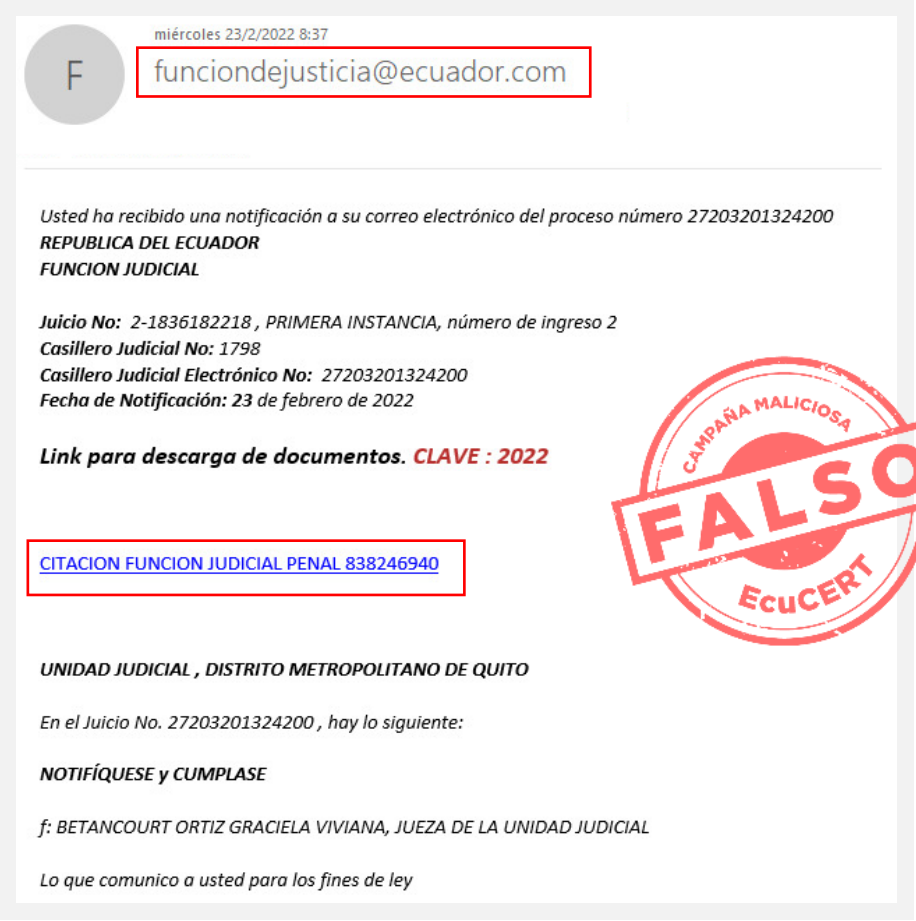

Figura 1.- ***Campaña maliciosa a nombre de función judicial***

Nro. Alerta:	EC-2022-18	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	04-mar-2022	**EcuCERT advierte nueva campaña de phishing "Función Judicial DMQ"**	V 1.0

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.
- 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.
- 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, sitios web desconocidos, etc.
- 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