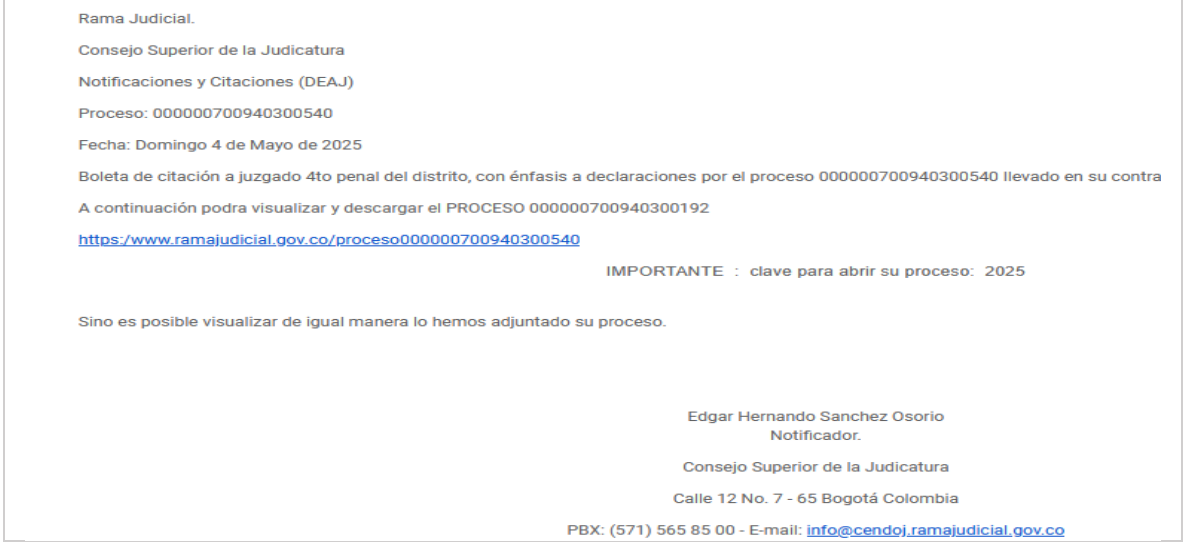
Mayo 12 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.msil/quasar
Cuenta de correo del remitente:	xiang.gao@theotino.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



Rama Judicial.

Consejo Superior de la Judicatura

Notificaciones y Citaciones (DEAJ)

Proceso: 00000700940300540

Fecha: Domingo 4 de Mayo de 2025

Boleta de citación a juzgado 4to penal del distrito, con énfasis a declaraciones por el proceso 00000700940300540 llevado en su contra

A continuación podra visualizar y descargar el PROCESO 00000700940300192

https:/www.ramajudicial.gov.co/proceso00000700940300540

IMPORTANTE : clave para abrir su proceso: 2025

Sino es posible visualizar de igual manera lo hemos adjuntado su proceso.

Edgar Hernando Sanchez Osorio
Notificador.

Consejo Superior de la Judicatura

Calle 12 No. 7 - 65 Bogotá Colombia

PBX: (571) 565 85 00 - E-mail: info@cendoj.ramajudicial.gov.co

El CSIRT Académico UNAD informa acerca de un asunto de ciberseguridad que ha sido identificado y abordado por este Equipo. Se ha detectado un evento de phishing dirigido a miembros de nuestra comunidad. Es preciso indicar que la técnica de Phishing es un tipo de ataque cibernético en el cual los adversarios intentan engañar a los usuarios para que se revele información confidencial, como contraseñas, números de tarjetas de crédito o información personal.

Se ha realizado la respectiva indagación y se han identificado una serie de indicadores de compromiso (IoCs) asociados con este asunto.

Indicadores de compromiso del archivo adjunto

Nombre del Archivo:	wwwramajudicialgovcoproceso00000070094030054066622 2.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	May 12, 2025 at 15:11:28
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections
MD5:	9C6E80206EFC1016BC25025D1BB09392
SHA1:	052E585D6A9EB715615C6C32B54F070B4E46B9F3

SHA256:	25129CB3E0EE9D2F6F77C5B80D2A2549418E2193EF20225DF445823407D76B0F
SSDEEP:	24576:5B/8z0UpHNTIPqBcoNTCmAUIklvNbB2A7uLqifnOkRfP995qGD2L/MEkUQQt q73Z:/8z0UpHNTIPqBcoNTCmAUI2NbB2A7uLW

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
C:\WINDOWS\system32\svchost.exe -k NetworkService -p -s Dnscache	C:\WINDOWS\system32\svchost.exe -k NetworkService -p -s Dnscache	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

CSIRT Académico UNAD
Correo electrónico: csirt@unad.edu.co
(+57 1) 344 37 00 Ext. 1042516