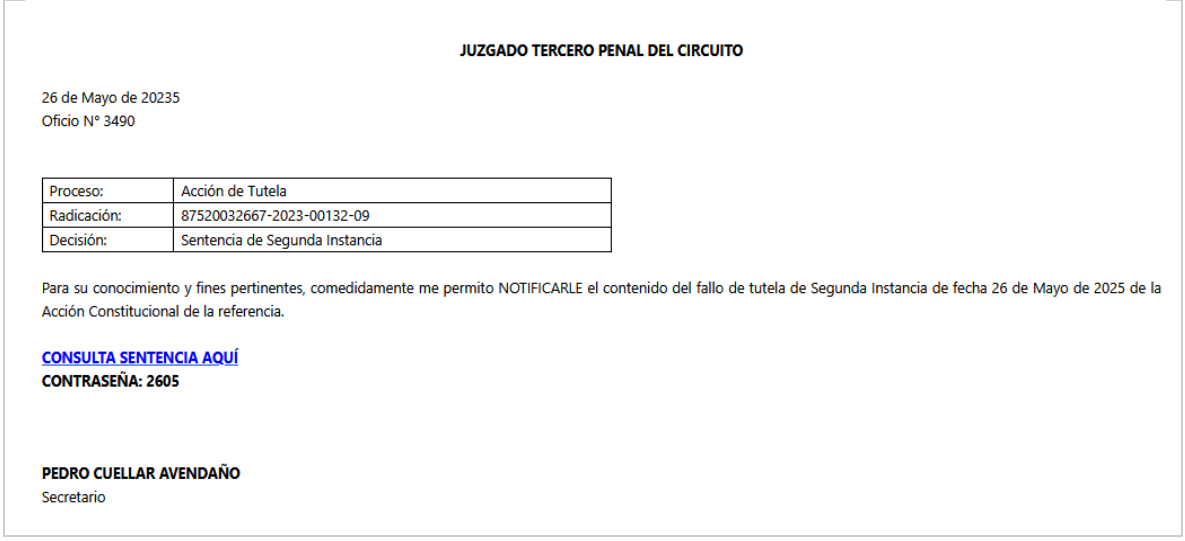
Mayo 26 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	Trojan:Win32/Sonbokli.A!cl.
Cuenta de correo del remitente:	almaceninduandes@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



JUZGADO TERCERO PENAL DEL CIRCUITO

26 de Mayo de 20235
Oficio N° 3490

Proceso:	Acción de Tutela
Radicación:	87520032667-2023-00132-09
Decisión:	Sentencia de Segunda Instancia

Para su conocimiento y fines pertinentes, comedidamente me permito NOTIFICARLE el contenido del fallo de tutela de Segunda Instancia de fecha 26 de Mayo de 2025 de la Acción Constitucional de la referencia.

CONSULTA SENTENCIA AQUÍ
CONTRASEÑA: 2605

PEDRO CUELLAR AVENDAÑO
Secretario

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:	26052025_895623215487445125548748544747485859693635214 5.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	May 26, 2025 at 19:23:59
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows, 6 sections
MD5:	12FD123A7E12414F1BC9C5640F9AA131
SHA1:	0E8DF69396A974E695DD72DF9F03C77E98C4D6F1

SHA256:	42ABD6F5D64579132C1AF15AE5D7502952E70A218AA3660D42F661816E2D397E
SSDEEP:	98304:61svXJG6gIS65IPDvyAA1UFmAeibzJMy6KsFWJrNPTuYLspzD5aeb3bIC7/O/yGE:o+blRjp33BgnrEPA5tYCXP4

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\26052025_895623215487445125548748544747485596936352145.exe"	"C:\Users\admin\AppData\Local\Temp\26052025_895623215487445125548748544747485596936352145.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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