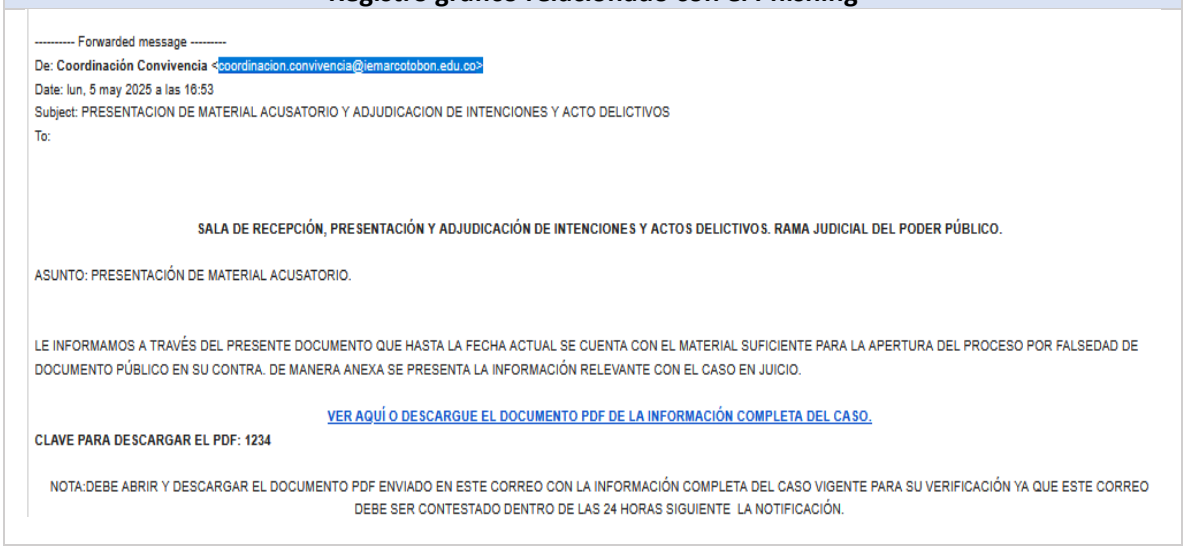
Mayo 07 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	downloader.ackb
Cuenta de correo del remitente:	coordinacion.convivencia@iemarcotobon.edu.co
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ---------
De: **Coordinación Convivencia** <coordinacion.convivencia@iemarcotobon.edu.co>
Date: lun, 5 may 2025 a las 16:53
Subject: PRESENTACION DE MATERIAL ACUSATORIO Y ADJUDICACION DE INTENCIONES Y ACTO DELICTIVOS
To:

SALA DE RECEPCIÓN, PRESENTACIÓN Y ADJUDICACIÓN DE INTENCIONES Y ACTOS DELICTIVOS. RAMA JUDICIAL DEL PODER PÚBLICO.

ASUNTO: PRESENTACIÓN DE MATERIAL ACUSATORIO.

LE INFORMAMOS A TRAVÉS DEL PRESENTE DOCUMENTO QUE HASTA LA FECHA ACTUAL SE CUENTA CON EL MATERIAL SUFICIENTE PARA LA APERTURA DEL PROCESO POR FALSEDAD DE DOCUMENTO PÚBLICO EN SU CONTRA. DE MANERA ANEXA SE PRESENTA LA INFORMACIÓN RELEVANTE CON EL CASO EN JUICIO.

VER AQUÍ O DESCARGUE EL DOCUMENTO PDF DE LA INFORMACIÓN COMPLETA DEL CASO.

CLAVE PARA DESCARGAR EL PDF: 1234

NOTA:DEBE ABRIR Y DESCARGAR EL DOCUMENTO PDF ENVIADO EN ESTE CORREO CON LA INFORMACIÓN COMPLETA DEL CASO VIGENTE PARA SU VERIFICACIÓN YA QUE ESTE CORREO DEBE SER CONTESTADO DENTRO DE LAS 24 HORAS SIGUIENTE LA NOTIFICACIÓN.

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:	Cam_Scanner_mayo#0505202510070000.js
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	May 07, 2025 at 09:57:16
MIME:	text/plain
Información del archivo:	Unicode text, UTF-8 text, with very long lines (487), with CRLF line terminators
MD5:	070DB3A1729E604F6B19B1339D84CA96

SHA1:	E9C1A8964119FADF79AA2A7B9894BB6168295942
SHA256:	BBFFAD27C461196ED26373C09B8C72753C1752D5C720F7CA8A1F24AE9B87396F
SSDEEP:	24:TZv6SdCLxbCp0EassjLCrlCL8He/TCLrPBCLNFCxm8w7:TUrspzassjGo6W+Q6xmf7

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Windows\System32\WScript.exe" C:\Users\admin\AppData\Local\Temp\Cam_Scanner_mayo#0505202510070000.js	"C:\Windows\System32\WScript.exe" C:\Users\admin\AppData\Local\Temp\Cam_Scanner_mayo#0505202510070000.js	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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