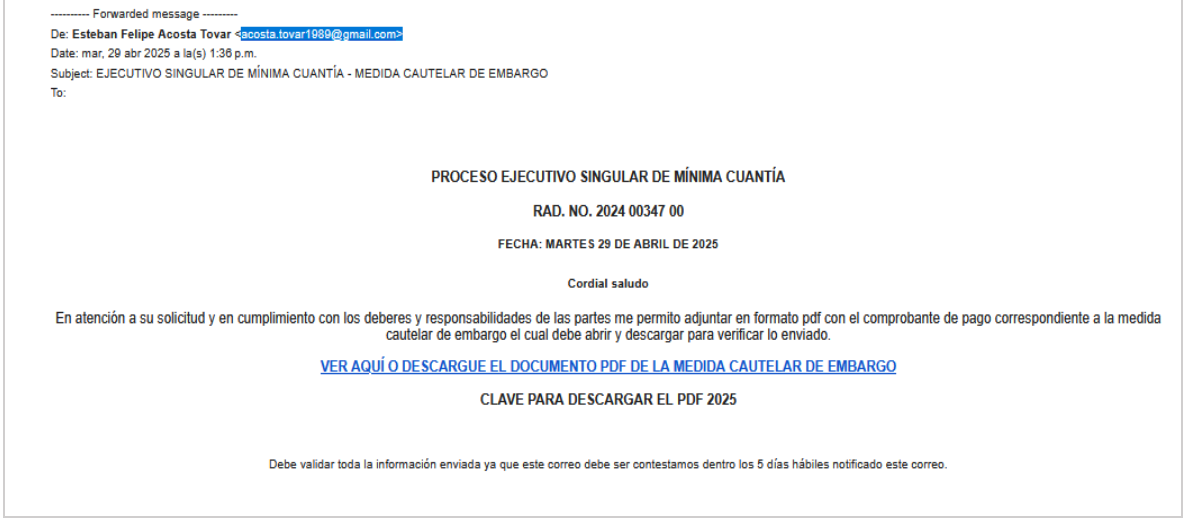
Abril 30 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	downloader.
Cuenta de correo del remitente:	acosta.tovar1989@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ---------
De: **Esteban Felipe Acosta Tovar** <acosta.tovar1989@gmail.com>
Date: mar, 29 abr 2025 a la(s) 1:36 p.m.
Subject: EJECUTIVO SINGULAR DE MÍNIMA CUANTÍA - MEDIDA CAUTELAR DE EMBARGO
To:

PROCESO EJECUTIVO SINGULAR DE MÍNIMA CUANTÍA

RAD. NO. 2024 00347 00

FECHA: MARTES 29 DE ABRIL DE 2025

Cordial saludo

En atención a su solicitud y en cumplimiento con los deberes y responsabilidades de las partes me permito adjuntar en formato pdf con el comprobante de pago correspondiente a la medida cautelar de embargo el cual debe abrir y descargar para verificar lo enviado.

VER AQUÍ O DESCARGUE EL DOCUMENTO PDF DE LA MEDIDA CAUTELAR DE EMBARGO

CLAVE PARA DESCARGAR EL PDF 2025

Debe validar toda la información enviada ya que este correo debe ser contestamos dentro los 5 días hábiles notificado este correo.

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:	DOCUMENTO PDF DE MEDIDA CAUTELAR DE EMBARGO ABRIL 2025.bat
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	April 30, 2025 at 10:01:05
MIME:	text/plain
Información del archivo:	ASCII text, with very long lines (60231), with CRLF, LF line terminators
MD5:	92d2cee7c863f0525e104819dd5ec4c0
SHA1:	04726a2ab1d0ddb0b5bb5bc018f7b88c79d7afbc
SHA256:	84ad9e363696c28a83ccb6bf9ff5250ddec7749f62346366ed78ea14277c78af

SSDEEP:	12:i7+oxzlk8zcsbebofd1hocj2h6x/v9qpxvvwpt280rwknjwfhcwn:i7nxnzcsmc8avewl3owyjwwwn

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
C:\WINDOWS\system32\cmd.exe /c ""C:\Users\admin\AppData\Local\Temp\DOCUMENTO PDF DE MEDIDA CAUTELAR DE EMBARGO ABRIL 2025.bat" "	C:\WINDOWS\system32\cmd.exe /c ""C:\Users\admin\AppData\Local\Temp\DOCUMENTO PDF DE MEDIDA CAUTELAR DE EMBARGO ABRIL 2025.bat" "	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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