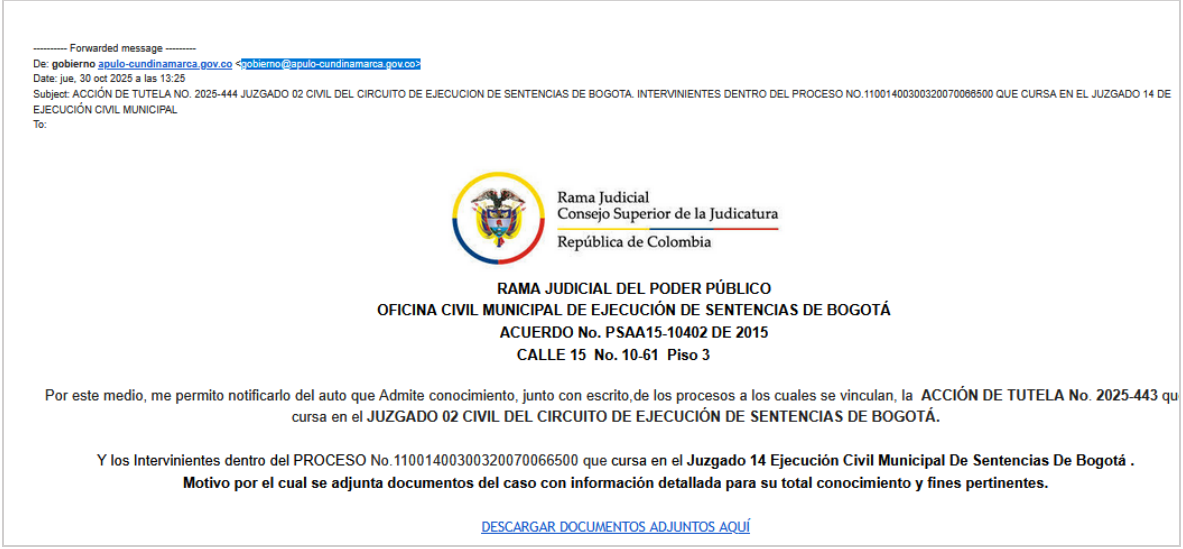
Octubre 31 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.
Cuenta de correo del remitente:	gobierno@apulo-cundinamarca.gov.co
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ---------
De: **gobierno** apulo-cundinamarca.gov.co <gobierno@apulo-cundinamarca.gov.co>
Date: jue, 30 oct 2025 a las 13:25
Subject: ACCIÓN DE TUTELA NO. 2025-444 JUZGADO 02 CIVIL DEL CIRCUITO DE EJECUCION DE SENTENCIAS DE BOGOTA. INTERVINIENTES DENTRO DEL PROCESO NO.11001400300320070066500 QUE CURSA EN EL JUZGADO 14 DE EJECUCIÓN CIVIL MUNICIPAL
To:

Rama Judicial
Consejo Superior de la Judicatura
República de Colombia

RAMA JUDICIAL DEL PODER PÚBLICO
OFICINA CIVIL MUNICIPAL DE EJECUCIÓN DE SENTENCIAS DE BOGOTÁ
ACUERDO No. PSAA15-10402 DE 2015
CALLE 15 No. 10-61 Piso 3

Por este medio, me permito notificarlo del auto que Admite conocimiento, junto con escrito,de los procesos a los cuales se vinculan, la **ACCIÓN DE TUTELA No. 2025-443** qu cursa en el **JUZGADO 02 CIVIL DEL CIRCUITO DE EJECUCIÓN DE SENTENCIAS DE BOGOTÁ.**

Y los Intervinientes dentro del PROCESO No.11001400300320070066500 que cursa en el **Juzgado 14 Ejecución Civil Municipal De Sentencias De Bogotá .**
Motivo por el cual se adjunta documentos del caso con información detallada para su total conocimiento y fines pertinentes.

DESCARGAR DOCUMENTOS ADJUNTOS AQUÍ

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.

Se realiza la verificación del archivo en mención, donde:

1. **El archivo no cuenta con ninguna protección mediante contraseña**: Para el usuario final, la ausencia de una contraseña en este tipo de archivos representa un alto riesgo. Al no estar protegido, el archivo puede ser abierto de manera inmediata, aumentando la probabilidad de que el usuario, sin sospechar de su naturaleza maliciosa, lo ejecute. Esto reduce significativamente el tiempo de reacción necesario para identificar la amenaza antes de que cause daño. Además, la facilidad de acceso elimina cualquier barrera

que pudiera obligar al usuario a detenerse y cuestionar la legitimidad del archivo, lo que incrementa el riesgo de infección y exposición de información sensible.

2. **El archivo descargado está comprimido y contiene un acceso directo malicioso**: Al extraer el archivo comprimido, se identificó un acceso directo que aparenta ser archivo legítimo, pero que, al analizar sus propiedades, se observa que es configurado para ejecutar acciones maliciosas. En la pestaña "Documento Web" del acceso directo, se encontró una URL con la siguiente dirección: file://\\62.60.226.168@80\file\dllhostt.exe

   Esta dirección apunta a un servidor remoto, desde el cual se intenta descargar y posiblemente ejecutar un archivo denominado build.exe. Este comportamiento indica un claro intento de los atacantes de explotar el acceso del usuario para conectarse a un recurso externo y ejecutar un archivo potencialmente malicioso.

   Para el usuario final, este tipo de ataque representa un riesgo crítico porque:

- **Ejecución inadvertida de malware**: El acceso directo puede ser engañosamente presentado como un archivo legítimo, aumentando la probabilidad de que el usuario lo abra sin sospechar de su naturaleza maliciosa.
- **Exposición a servidores maliciosos**: Al intentar acceder a la dirección especificada, el sistema del usuario podría exponer información como la dirección IP o credenciales de red, facilitando un ataque más amplio.
- **Automatización del proceso malicioso**: La configuración del acceso directo permite que la descarga y ejecución del archivo se realice de manera rápida y silenciosa, sin intervención adicional del usuario, reduciendo las posibilidades de detección temprana.

Indicadores de compromiso del archivo adjunto

Nombre del Archivo:	DOCUMENTO DE TUTELA NO. 2025-444 JUZGADO 02 CIVIL DEL CIRCUITO DE EJECUCION DE SENTENCIAS DE BOGOTA. INTERVINIENTES DENTRO DEL PROCESO NO.11001400300320070066500 QUE CURSA EN EL JUZGADO 14 DE EJECUCIÓN CIVIL M.url
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	October 31, 2025 at 10:52:42
MIME:	application/x-wine-extension-ini
Información del archivo:	Generic INItialization configuration [InternetShortcut]
MD5:	6D57DF1EA177D928AB886312D88336AC
SHA1:	8CA8EDAB78095105F3EB3B837E23EDB77242A008
SHA256:	6D1E5BBF82D4B2CF11126689B4702922B517E249943DD92C184AA7E44920EEE0
SSDEEP:	6:JyXSvVG/FTVmJtOFJb5if5oeTckmrISDXAWYosv:cXaVWfmJtOFJQRzgrDXo

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\WINDOWS\system32\rundll32.exe" "C:\WINDOWS\system32\ieframe.dll",OpenURL %l	"C:\WINDOWS\system32\rundll32.exe" "C:\WINDOWS\system32\ieframe.dll",OpenURL %l	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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