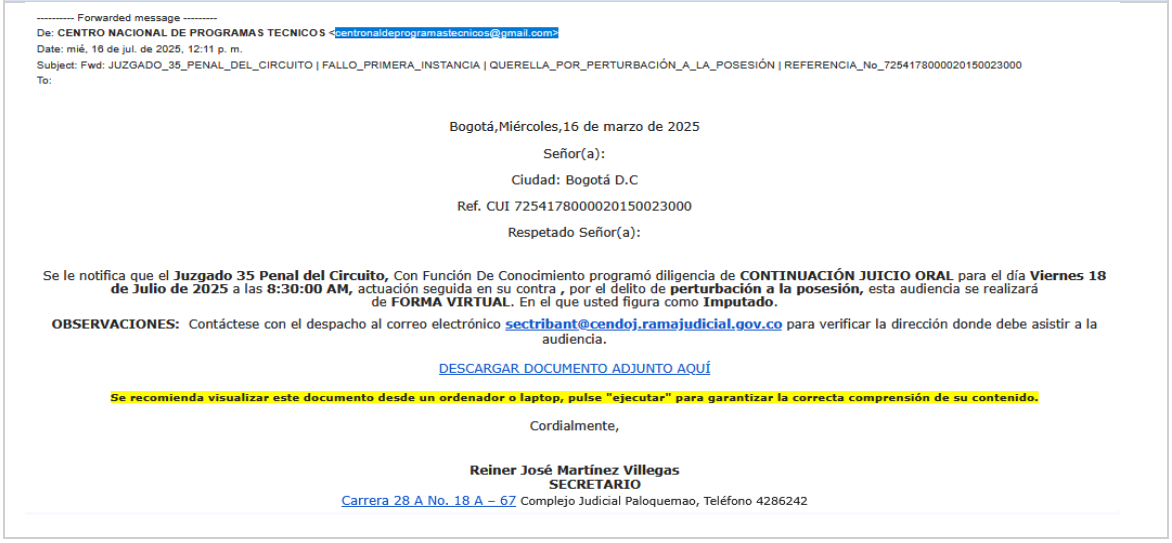
Julio 18 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

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



--------- Forwarded message ---------
De: **CENTRO NACIONAL DE PROGRAMAS TECNICOS** <centronaldeprogramastecnicos@gmail.com>
Date: mié, 16 de jul. de 2025, 12:11 p. m.
Subject: Fwd: JUZGADO_35_PENAL_DEL_CIRCUITO | FALLO_PRIMERA_INSTANCIA | QUERELLA_POR_PERTURBACIÓN_A_LA_POSESIÓN | REFERENCIA_No_72541780000201500230000
To:

Bogotá,Miércoles,16 de marzo de 2025

Señor(a):

Ciudad: Bogotá D.C

Ref. CUI 72541780000201500230000

Respetado Señor(a):

Se le notifica que el **Juzgado 35 Penal del Circuito,** Con Función De Conocimiento programó diligencia de **CONTINUACIÓN JUICIO ORAL** para el día **Viernes 18 de Julio de 2025** a las **8:30:00 AM,** actuación seguida en su contra **,** por el delito de **perturbación a la posesión,** esta audiencia se realizará de **FORMA VIRTUAL**. En el que usted figura como **Imputado**.

OBSERVACIONES: Contáctese con el despacho al correo electrónico **sectribant@cendoj.ramajudicial.gov.co** para verificar la dirección donde debe asistir a la audiencia.

DESCARGAR DOCUMENTO ADJUNTO AQUÍ

Se recomienda visualizar este documento desde un ordenador o laptop, pulse "ejecutar" para garantizar la correcta comprensión de su contenido.

Cordialmente,

Reiner José Martínez Villegas
SECRETARIO
Carrera 28 A No. 18 A – 67 Complejo Judicial Paloquemao, Teléfono 4286242

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://\\176.46.152.39@80\file\FoxitPDFEditor.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:	IMG - 000929848855 JUZGADO_35_PENAL_DEL_CIRCUITO FALLO_PRIMERA_INSTANCIA QUERELLA_POR_PERTURBACIÓN_A_LA_POSESIÓN REFERENCIA_No_72541780000201500230000 (1).url
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	July 18, 2025 at 11:10:10
MIME:	application/x-wine-extension-ini
Información del archivo:	Generic INItialization configuration [InternetShortcut]
MD5:	4919349C02394CD5AD8AED7EC90C748D
SHA1:	22F31CDAFE295ADB5BDF5349BF89E8BC56288DA4
SHA256:	0FFA4E0DFD45020C619D55D0FE84F397CA6ADAF2D6E4DDF69FF3A63DBE98ECB3
SSDEEP:	6:JyXSvVG/FTVmJtOFJb5if5oeTckmr85vPqdl/kNQsv:cXaVWfmJtOFJQRzgomFkN

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