



## Boletín de Ciberseguridad

Junio 11 de 2025

### COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

|  |  |
|--|--|
| <b>Técnica Mitre:</b>                  | Phishing   |
| <b>Malware detectado:</b>              | trojan.  |
| <b>Cuenta de correo del remitente:</b> | <a href="mailto:rafaelriverajimenez@gmail.com">rafaelriverajimenez@gmail.com</a> |
| <b>TLP:</b>                            | BLANCO   |

**Registro grafico relacionado con el Phishing**

----- Forwarded message -----  
 De: rafael rivera <[rafaelriverajimenez@gmail.com](mailto:rafaelriverajimenez@gmail.com)>  
 Date: mié, 11 jun 2025, 9:57 a. m.  
 Subject: Querrela por perturbación a la posesión - Señalamiento fiscal 11 de Junio  
 To:



Juzgado 29 de Familia Bogotá D.C - Ref CUI No. 0000003852116678920249655487  
**Ref CUI No. 0000003852116678920249655487**  
 Fecha: 11/06/2025  
 Asunto: Querrela por perturbación a la posesión  
 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



## Boletín de Ciberseguridad

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://\62.60.226.165@80\file\PortafolioPDF.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

|                                 |  |
|---------------------------------|--|
| <b>Nombre del Archivo:</b>      | Documento por perturbación a la posesión - Señalamiento fiscal 11 de Junio.url |
| <b>Veredicto:</b>               | <b>Actividad sospechosa</b>  |
| <b>Fecha del análisis:</b>      | June 11, 2025 at 12:10:28  |
| <b>MIME:</b>                    | application/x-wine-extension-ini   |
| <b>Información del archivo:</b> | Generic INtialization configuration [InternetShortcut]                         |
| <b>MD5:</b>                     | CB8FDFCB193745DAEE0F3ADDE9F8D8C1   |
| <b>SHA1:</b>                    | E2DC741F5BC8CD0AD30CD35D051A88F844062DA9                                       |
| <b>SHA256:</b>                  | FF5C206C79BB64015862404D9CCA0B519D7CD32C13AD4985A0C52FDC8B17DEFB               |
| <b>SSDEEP:</b>                  | 6:JyXSvVG/FTVmJtOFJb5if5oeTckmrlST//6vosv:cXaVWfmJtOFJQRzgr7/6L                |

Fuente. CSIRT Académico UNAD

### Información de proceso



## Boletín de Ciberseguridad

| CMD                                | Ruta Comprometida                  | Proceso Padre |
|------------------------------------|------------------------------------|---------------|
| "C:\WINDOWS\system32\rundll32.exe" | "C:\WINDOWS\system32\rundll32.exe" | explorer.exe  |

Fuente. CSIRT Académico UNAD

Cordialmente

### CSIRT Académico UNAD

Correo electrónico: [csirt@unad.edu.co](mailto:csirt@unad.edu.co)

(+57 1) 344 37 00 Ext. 1042516