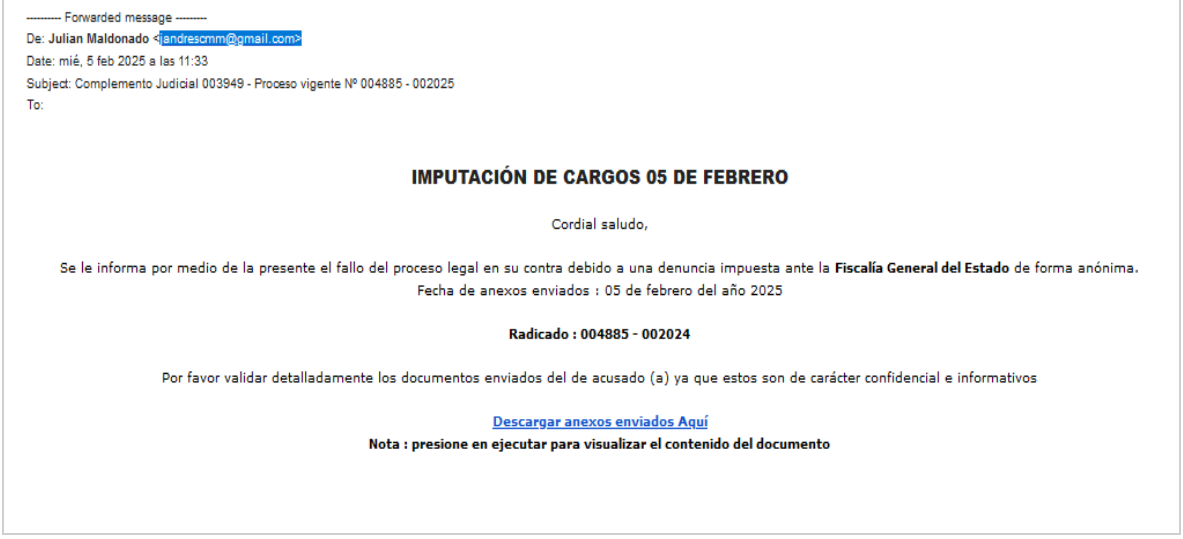
Enero 06 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

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



---------- Forwarded message ---------
De: **Julian Maldonado** <jandrescmm@gmail.com>
Date: mié, 5 feb 2025 a las 11:33
Subject: Complemento Judicial 003949 - Proceso vigente Nº 004885 - 002025
To:

IMPUTACIÓN DE CARGOS 05 DE FEBRERO

Cordial saludo,

Se le informa por medio de la presente el fallo del proceso legal en su contra debido a una denuncia impuesta ante la **Fiscalía General del Estado** de forma anónima.
Fecha de anexos enviados : 05 de febrero del año 2025

Radicado : 004885 - 002024

Por favor validar detalladamente los documentos enviados del de acusado (a) ya que estos son de carácter confidencial e informativos

Descargar anexos enviados Aquí
Nota : presione en ejecutar para visualizar el contenido del documento

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 un archivo legítimo, pero que, al analizar sus propiedades, se observó que está configurado para ejecutar una acción maliciosa. En la pestaña "Documento Web" del acceso directo, se encontró una URL con la siguiente dirección: file://\\62.60.226.64@80\file\8377_9619.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 Judicial 003949 - Proceso vigente Nº 004885 - 002025.url
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	February 06, 2025 at 17:48:02
MIME:	application/x-wine-extension-ini
Información del archivo:	Generic INItialization configuration [InternetShortcut]
MD5:	16D89ABA9A671A47CEF29DEFBBAFC5BE
SHA1:	6A319C68B03B03522C631FB43EB7AD2909742710
SHA256:	FC2E0C74F76A40C8469F14C8D8E681B1A112C05343BC5F819A7801DD436C3BA9
SSDEEP:	6:JyXSvVG/FTVmJtOFJb5if5oeTckmrIoXYwsv:cXaVWfmJtOFJQRzgXXYr

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