Mayo 14 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.
Cuenta de correo del remitente:	carogorojas@gmail.com
TLP:	**BLANCO**

Registro grafico relacionado con el Phishing

---------- Forwarded message ---------
De: **Carolina Gomez Muak** <carogorojas@gmail.com>
Date: mar, 13 may 2025 a las 10:10
Subject: DICTAMEN DE PROCESO PENAL No. CUI 158616000129-2025-0215541305
To:

REPÚBLICA DE COLOMBIA
RAMA JUDICIAL DEL PODER PÚBLICO
JUZGADO QUINTO ADMINISTRATIVO ORAL DEL CIRCUITO JUDICIAL
89488441485.png

Respetado señor(a)

REFERENCIA EXPEDIENTE No. 158616000129

La presente demanda pretende que se declare administrativa y patrimonialmente responsables a la **NACIÓN - RAMA JUDICIAL - FISCALÍA GENERAL DE LA NACIÓN** de los daños y perjuicios causados a los demandantes con la privación injusta y falsificación demanda documento público y privado.

VER AQUÍ O DESCARGAR EN LA PARTE DE ABAJO PDF DONDE SE ANEXA DOCUMENTO DE DENUNCIA

CLAVE SEGURA A PDF: 1306

La presente gestión ha sido efectuada en cumplimiento de los requisitos legales vigentes y se encuentra registrada bajo el número anteriormente indicado, correspondiente al mes de abril, si aplica.

--
Néstor Henry Cáceres Solano.
Líder Registro y Control UNAD Zona Centro Oriente.
Tel. 6358577 ext. 1047005-1047006
Bucaramanga.

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:	ARCHIV_PDF_1305_1111_777_125555456922563286565 5KJ DVJNBHBSXC.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	May 14, 2025 at 16:27:01
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows, 7 sections
MD5:	CBAB12848F7C40552D33AA5C66AF27C3
SHA1:	08F51CA19729620682ACB51859BA12A4108CE6F9
SHA256:	903D746BFE35949669C52734359A07E024F04B1DBD1F9FE009331B79A2DC872F

SSDEEP:	98304:m/9ADTpciOAw+m+/feFxlJoxAhjoUm6wMrgAHQEFBtiCG92s/Za0by5RioKgmI4p:wZseoEUKQHSqMehhtNV

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\{DA8F6A25-5CB7-4B58-AA55-954FF3CC8D74}\.cr\ARCHIV_PDF_1305_1111_777_125555456992563286555KJDVJNBHBSXC.exe" -burn.clean.room="C:\Users\admin\AppData\Local\Temp\ARCHIV_PDF_1305_1111_777_125555456992563286555KJDVJNBHBSXC.exe" -burn.filehandle.attached=664 -burn.filehandle.self=688	"C:\Users\admin\AppData\Local\Temp\{DA8F6A25-5CB7-4B58-AA55-954FF3CC8D74}\.cr\ARCHIV_PDF_1305_1111_777_125555456992563286555KJDVJNBHBSXC.exe" -burn.clean.room="C:\Users\admin\AppData\Local\Temp\ARCHIV_PDF_1305_1111_777_125555456992563286555KJDVJNBHBSXC.exe" -burn.filehandle.attached=664 -burn.filehandle.self=688	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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