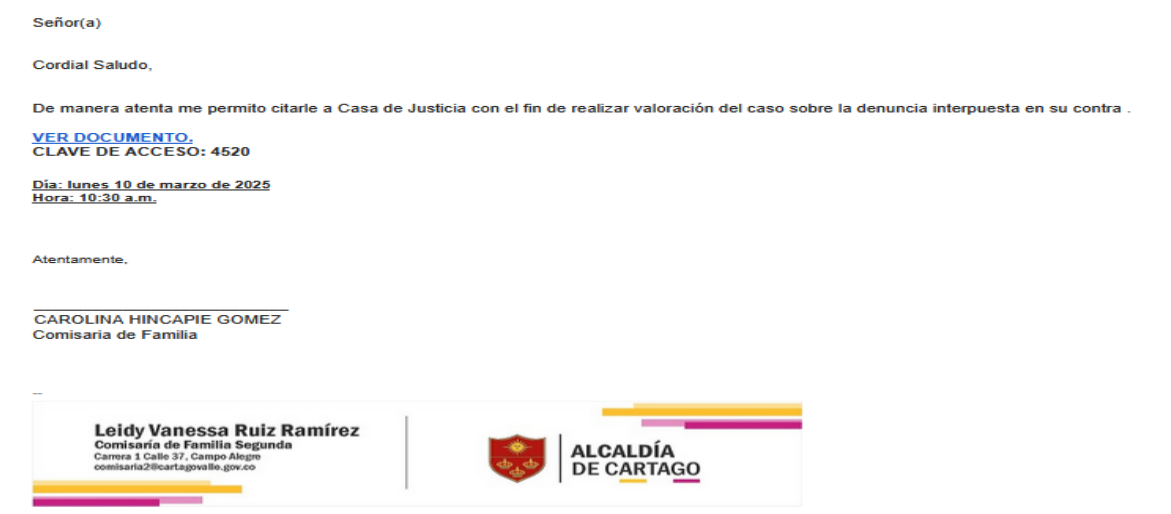
Febrero 26 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.
Cuenta de correo del remitente:	apre777@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



Señor(a)

Cordial Saludo,

De manera atenta me permito citarle a Casa de Justicia con el fin de realizar valoración del caso sobre la denuncia interpuesta en su contra .

VER DOCUMENTO.
CLAVE DE ACCESO: 4520

Dia: lunes 10 de marzo de 2025
Hora: 10:30 a.m.

Atentamente,

CAROLINA HINCAPIE GOMEZ
Comisaria de Familia

Leidy Vanessa Ruiz Ramírez
Comisaría de Familia Segunda
Carrera 1 Calle 37, Campo Alegre
comisaria2@cartagovalle.gov.co

ALCALDÍA DE CARTAGO

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:	DOCX-1458-7415-1025-41587-595-22025.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	February 26, 2025 at 16:43:59
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32+ executable (GUI) x86-64, for MS Windows, 6 sections
MD5:	2A39AB7049226DEC986FA602A26F5372

SHA1:	F0BAF3B4F1DBCC6DD21E6F1279C741C0051C03CC
SHA256:	AD4CD780BD7ACCD7482DCF6222910AAFEE971C7AB870EBAE0022D51B237FA5CB
SSDEEP:	6144:HKmvtb65ZrPmkHkpz1nJFRH//blmTRr5Hy40Zi3H5IeLeK:3IHkh1nPRH3blmRr5Hy5ZuIMf

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\DOCX-1458-7415-1025-41587-595-22025.exe"	"C:\Users\admin\AppData\Local\Temp\DOCX-1458-7415-1025-41587-595-22025.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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