Agosto 22 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	Scr.MalSvg!gen2
Cuenta de correo del remitente:	ddiaz536@unab.edu.co
TLP:	**BLANCO**

Registro grafico relacionado con el Phishing

---------- Forwarded message ---------
De: **DIANA MILENA DIAZ MASMELA** <ddiaz536@unab.edu.co>
Date: mié, 20 ago 2025 a la(s) 2:50 p.m.
Subject: Información tutelar en su contra con Ref# 4578804962 MG1220
To:

FISCALIA
GENERAL DE LA NACION

FISCALÍA GENERAL DE LA NACIÓN

Respetado (a),

A través de la presente me permito notificarle de manera muy respetuosa la siguiente citación de manera presencial para tratar de establecer cuáles fueron los hechos que ocasionaron el delito de calumnia, de la cual se le acusa dentro el consejo de la judicatura distrital, de acuerdo a lo concebido en el art 024 de la ley 0413 de 1991 deberá hacer acto de presencia y bajo juramento relatar con la verdad lo sucedido.

Detalles De La Citación Extrajudicial
Clave de acceso: MG1220

CAMILA SOFIA BUITRAGO VELEZ
Abogada y Asesora Jurídica

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:	Información tutelar en su contra con Ref# 4578804962.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	August 22, 2025 at 09:40:28
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32+ executable (GUI) x86-64, for MS Windows, 6 sections
MD5:	16F09DFA13BDB0226DB880FF6DD635BD
SHA1:	093FBD7BEB9183DF9F8A196F436669A8A923C3C3

SHA256:	AD0AC92587839E6F802B43E5EBA46A4314DA2075608BBC484201A56C8C4B4B5F
SSDEEP:	98304:pLn6i232c20YXbsJk8EJl64Nj+1do1r6GXPOliriGnH5UvKC13z73uUJclk+MCGN:jlRbWWi9gshP

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
C:\WINDOWS\System32\slui.exe -Embedding	C:\WINDOWS\System32\slui.exe -Embedding	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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