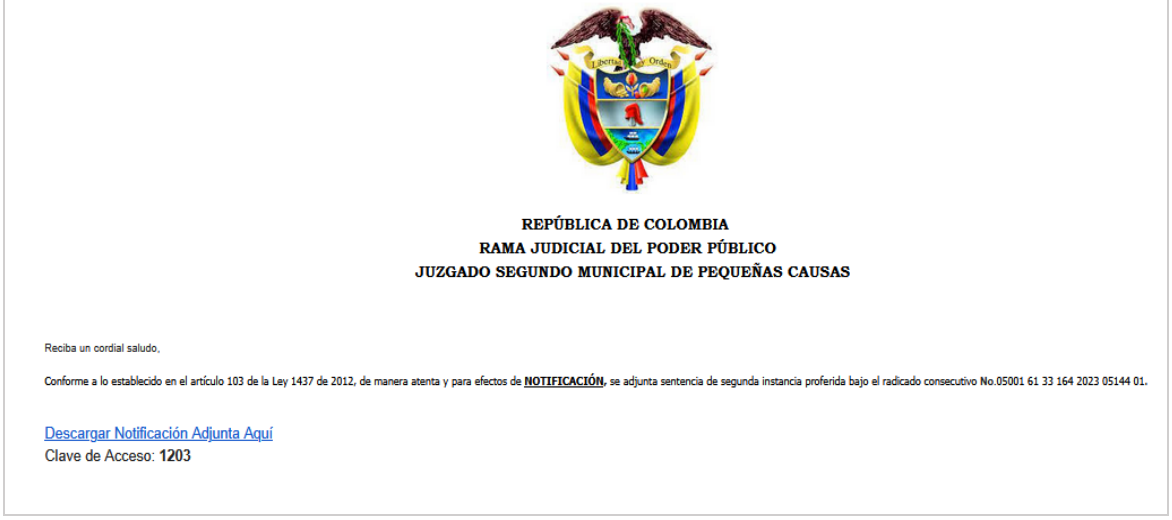
Marzo 14 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

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



REPÚBLICA DE COLOMBIA
RAMA JUDICIAL DEL PODER PÚBLICO
JUZGADO SEGUNDO MUNICIPAL DE PEQUEÑAS CAUSAS

Reciba un cordial saludo,

Conforme a lo establecido en el artículo 103 de la Ley 1437 de 2012, de manera atenta y para efectos de **NOTIFICACIÓN**, se adjunta sentencia de segunda instancia proferida bajo el radicado consecutivo No.05001 61 33 164 2023 05144 01.

Descargar Notificación Adjunta Aquí
Clave de Acceso: **1203**

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:	1203_1220_DOCU_FACT_OFX_POIU_7896523147.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	March 14, 2025 at 20:23:57
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32+ executable (GUI) x86-64, for MS Windows, 7 sections
MD5:	3E1F7529AE3A5534CFAEC4A3AA8BB750
SHA1:	21289A1AB17E98B8DA77E9EDB60A3260ADEAE0BF

SHA256:	EB1B7B9339B349202CE8498202B995C61FFD1BA322A3AC4AA8B7B67FB666DA16
SSDEEP:	24576:h+068/kwZc6ykoj3Mr/9a4fnBdaIaZdIZ2:h+06ok+bho7Mr/9a4fnBdaj

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\1203_1220_DOCU_FACT_OFX_POIU_7896523147.exe"	"C:\Users\admin\AppData\Local\Temp\1203_1220_DOCU_FACT_OFX_POIU_7896523147.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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