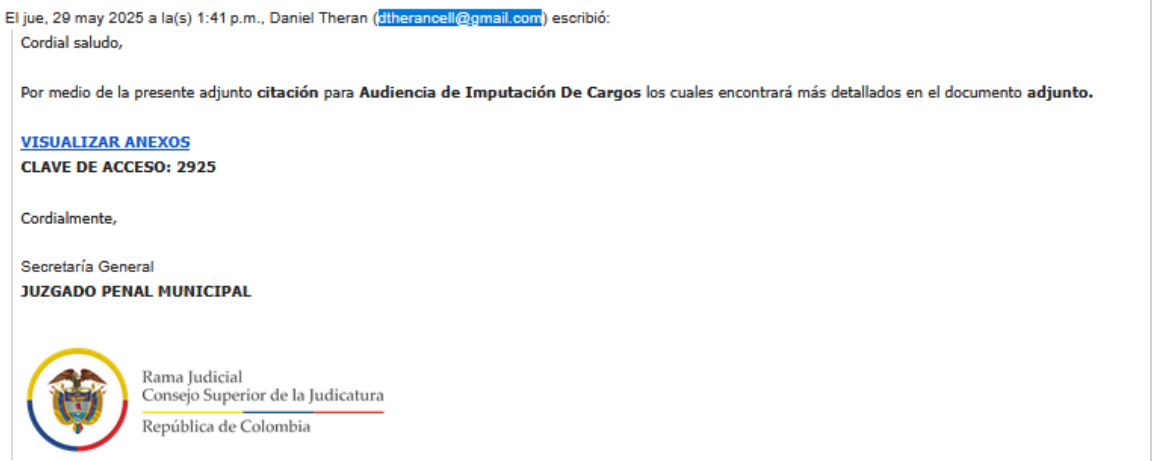
Mayo 29 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

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



El jue, 29 may 2025 a la(s) 1:41 p.m., Daniel Theran (dtherancell@gmail.com) escribió:

Cordial saludo,

Por medio de la presente adjunto **citación** para **Audiencia de Imputación De Cargos** los cuales encontrará más detallados en el documento **adjunto.**

VISUALIZAR ANEXOS
CLAVE DE ACCESO: 2925

Cordialmente,

Secretaría General
JUZGADO PENAL MUNICIPAL

Rama Judicial
Consejo Superior de la Judicatura
República de Colombia

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:	not0000077954tr651-R65779101065165E46815561-8461651-TED565464165-SEM66151864616465411T5-4896Y484646511638498794641488-69651651TYU1681-BNU616516NUM6518965164546151V684664FIN6.vbs
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	May 29, 2025 at 16:44:51
MIME:	text/plain
Información del archivo:	Unicode text, UTF-8 text, with CRLF line terminator
MD5:	BEF84E24A10859EB22C1DDF9376BB583

SHA1:	0458AEF889686449622054ACFAF639D7E5F8FF1D
SHA256:	F98B49AA5EC566EF5F075F0BB56D0ECE3B6752A9CAED873633DFA833E44A7BED
SSDEEP:	768:PDi5H/CZok5RU4NkXzzZq3WnHAazo8eaPa5BEfEMWrKCVLKr:PDi5H/CZoxqQaTVLKr

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\WINDOWS\System32\OpenWith.exe" C:\Users\admin\AppData\Local\Temp\bd7abd23-4b90-4352-8cc0-4654f028124f.vba	"C:\WINDOWS\System32\OpenWith.exe" C:\Users\admin\AppData\Local\Temp\bd7abd23-4b90-4352-8cc0-4654f028124f.vba	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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