Mayo 19 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.
Cuenta de correo del remitente:	jorgejorgejorge14@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	

---------- Forwarded message ---------
De: **Jorge Andres Torres** <jorgejorgejorge14@gmail.com>
Date: lun, 19 may 2025 a la(s) 9:04 a.m.
Subject: OFICIO CITACIÓN AUDIENCIA REF; P-2023-00529681;
To:

Consejo Superior de la Judicatura

JUZGADO PROMISCUO MUNICIPAL

P-2023-00529681

Cordial saludo;

Por medio del presente me permito remitir adjunto Oficio No. 8614-051-1593-2023. Del proceso en referencia.

CONSULTAR OFICIO AQUÍ
CONTRASEÑA: 1905

Atentamente,

Susana Urrutia Pelaez
Citadora

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:	DOCUMENTO_00001111_879985445822562232326598562659865.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	May 19, 2025 at 12:19:03
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32+ executable (GUI) x86-64, for MS Windows, InstallShield self-extracting archive, 9 sections
MD5:	43468419FEE8EE89FBC7F0D2ECE3C97D
SHA1:	5DE64AF4E77DBBDE29B1653D16BA6163741643A5

SHA256:	9841B2B0EEDD10CA072DED35EB49117B5941378996C3DD4D3CD3B6DE50087763
SSDEEP:	98304:wSdDQecsFyqtCerQPoSCqsHbQha54pblQbLw+iX6lk9rImwXEaGxgUSLelkrSgzd:vUmZF8Yf0G

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\{D14ED76C-D460-4E27-A0CD-B218DAAA101A}\.cr\DOCUMENTO_00001111_879985445822562232326598562659865.exe" -burn.clean.room="C:\Users\admin\AppData\Local\Temp\DOCUMENTO_00001111_879985445822562232326598562659865.exe" -burn.filehandle.attached=616 -burn.filehandle.self=684	"C:\Users\admin\AppData\Local\Temp\{D14ED76C-D460-4E27-A0CD-B218DAAA101A}\.cr\DOCUMENTO_00001111_879985445822562232326598562659865.exe" -burn.clean.room="C:\Users\admin\AppData\Local\Temp\DOCUMENTO_00001111_879985445822562232326598562659865.exe" -burn.filehandle.attached=616 -burn.filehandle.self=684	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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