Enero 28 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.
Cuenta de correo del remitente:	javierfernandoreyesrodriguez2@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	

---------- Forwarded message ---------
De: **Javier fernando Reyes Rodriguez** <javierfernandoreyesrodriguez2@gmail.com>
Date: mar, 28 ene 2025 a la(s) 9:15 a.m.
Subject: PRELUDIO PARA CITACIÓN JUDICIAL RAD. N° 0094858356
To:

FISCALÍA GENERAL DE LA NACIÓN
JUZGADO PROMISCUO DEL SECTOR PÚBLICO

A través del presente documento damos el conocimiento a usted de la instauración formal de denuncia N° 0094858356 por los hechos de **Falsedad de documentos.**

De manera anexa encontrará los detalles y componentes que han dado lugar a la denuncia que hoy lo aqueja, dando lugar a esta situación de carácter judicial.

Por lo anterior le solicitamos verificar las fechas y plazos establecidos dentro del archivo adjunto.

VER AQUÍ O DESCARGAR ARCHIVO ADJUNTO AL FINAL DE DOCUMENTO
CÓDIGO DE ACCESO 3220

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:	PRELUDIO PARA CITACIÓN JUDICIAL RAD. N° 0094858356.vbe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	January 28, 2025 at 17:45:54
MIME:	application/octet-stream
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows, 6 sections
MD5:	4B9FE4771AF6F42DBEF5217BAC3D2A5E
SHA1:	34F8E9147248AFA4029F7AFF77DB7FE8E2FF7727
SHA256:	506D9EC787ABE50B37C9B4ED0A0976CD6B3D9A465633EBA9327ABE8A94ABAE80

SSDEEP:	192:PawyKhUwTxasWjA9pXqQNdKlzzw6As9QOK:ZyDwTxasWOpXqQKFwVz

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Program Files\VideoLAN\VLC\vlc.exe" --started-from-file "C:\Users\admin\AppData\Local\Temp\PRELUDIO PARA CITACIÓN JUDICIAL RAD. N° 0094858356.vbe.mp3"	"C:\Program Files\VideoLAN\VLC\vlc.exe" --started-from-file "C:\Users\admin\AppData\Local\Temp\PRELUDIO PARA CITACIÓN JUDICIAL RAD. N° 0094858356.vbe.mp3"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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