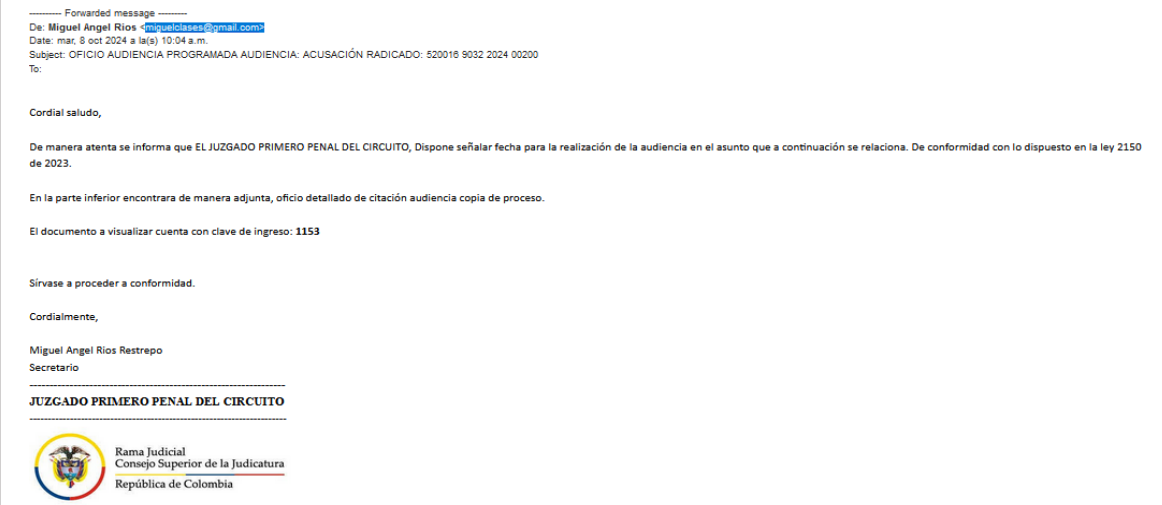
Octubre 08 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

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



---------- Forwarded message ---------
De: **Miguel Angel Rios** <miguelclases@gmail.com>
Date: mar, 8 oct 2024 a la(s) 10:04 a.m.
Subject: OFICIO AUDIENCIA PROGRAMADA AUDIENCIA: ACUSACIÓN RADICADO: 520016 9032 2024 00200
To:

Cordial saludo,

De manera atenta se informa que EL JUZGADO PRIMERO PENAL DEL CIRCUITO, Dispone señalar fecha para la realización de la audiencia en el asunto que a continuación se relaciona. De conformidad con lo dispuesto en la ley 2150 de 2023.

En la parte inferior encontrara de manera adjunta, oficio detallado de citación audiencia copia de proceso.

El documento a visualizar cuenta con clave de ingreso: **1153**

Sírvase a proceder a conformidad.

Cordialmente,

Miguel Angel Rios Restrepo
Secretario

JUZGADO PRIMERO PENAL DEL CIRCUITO

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:	Ab5200119032202400200519982037l5.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	October 08, 2024 at 11:56:04
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	34EE6B8D2C0578E18DD75C52678B81CE
SHA1:	6D552C784B281B8587D7E17E0C59B4D997A654E9
SHA256:	D41F8AE0DF709B0243DB420707A5D87D45EEC903AD2FDA40A03963B958F83A18

SSDEEP:	98304:R/H96qYa9DMj6r/Kf1ZvXQUHdxybzbBrsX4CgnBmQ3HMwy7mvCaw4r2n:Dzr3RxI

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\Ab5200119032202400200519982037 15.exe"	"C:\Users\admin\AppData\Local\Temp\Ab5200119032202400200519982037 15.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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