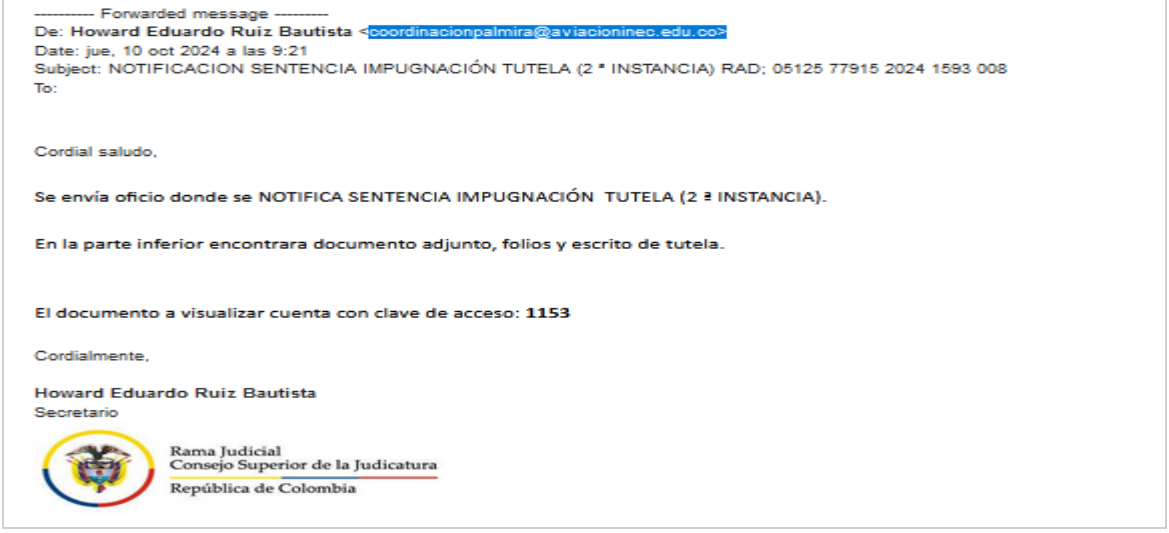
Octubre 11 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.generickds
Cuenta de correo del remitente:	coordinacionpalmira@aviacioninec.edu.co
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ---------
De: **Howard Eduardo Ruiz Bautista** <coordinacionpalmira@aviacioninec.edu.co>
Date: jue, 10 oct 2024 a las 9:21
Subject: NOTIFICACION SENTENCIA IMPUGNACIÓN TUTELA (2 ª INSTANCIA) RAD: 05125 77915 2024 1593 008
To:

Cordial saludo,

Se envía oficio donde se NOTIFICA SENTENCIA IMPUGNACIÓN TUTELA (2 ª INSTANCIA).

En la parte inferior encontrara documento adjunto, folios y escrito de tutela.

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

Cordialmente,

Howard Eduardo Ruiz Bautista
Secretario

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:	OFX1159ImpuganaTutelaRadicado05125 77915 2024 1593 008.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	October 11, 2024 at 14:03:31
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	a10ca62ac21d9d838ee398f0a0dd2198
SHA1:	2876246883c50d16662d8bfd1451154267c1c7e3
SHA256:	ff4a8be4e90fd047718103a1527a2d0a452f76fdbd2c18de9d98d7c2ab4926c6

SSDEEP:	196608:qFltqUFFD+Uo2jWZBvJ8cQhjMUsd81ZdP:05FFD+UNjWZBIhNZl

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\<USER>\Desktop\OFX1159ImpugnaTutelaRadicado05125 77915 2024 1593 008.exe"	"C:\Users\<USER>\Desktop\OFX1159ImpugnaTutelaRadicado05125 77915 2024 1593 008.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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