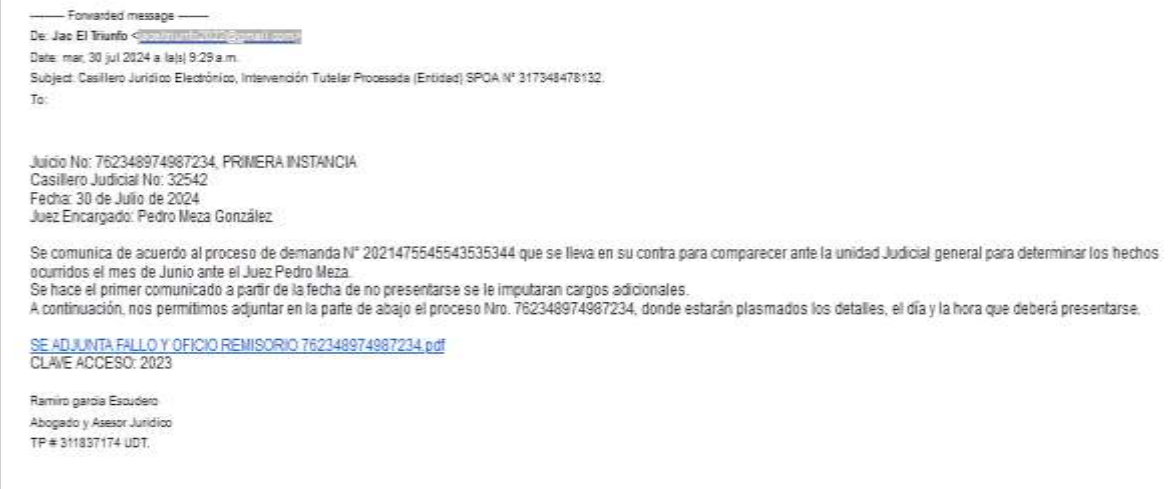
Julio 31 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.lazy/remcos
Cuenta de correo del remitente:	jaceltriunfo2022@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



——— Forwarded message ———
De: Jac El Triunfo <[redacted]>
Date: mar, 30 jul 2024 a la(s) 9:29 a.m.
Subject: Casillero Juridico Electrónico, Intervención Tutelar Procesada (Entidad) SPOA N° 317348478132.
To:

Juicio No: 762348974987234, PRIMERA INSTANCIA
Casillero Judicial No: 32542
Fecha: 30 de Julio de 2024
Juez Encargado: Pedro Meza González

Se comunica de acuerdo al proceso de demanda N° 2021475545543535344 que se lleva en su contra para comparecer ante la unidad Judicial general para determinar los hechos ocurridos el mes de Junio ante el Juez Pedro Meza.
Se hace el primer comunicado a partir de la fecha de no presentarse se le imputaran cargos adicionales.
A continuación, nos permitimos adjuntar en la parte de abajo el proceso Nro. 762348974987234, donde estarán plasmados los detalles, el día y la hora que deberá presentarse.

SE ADJUNTA FALLO Y OFICIO REMISORIO 762348974987234.pdf
CLAVE ACCESO: 2023

Ramiro garcia Escudero
Abogado y Asesor Juridico
TP # 311837174 UDT.

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:	Ficha_Tecnica_Juridica_N°_417394813..exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Julio 31, 2024 at 14:30:29
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	4E875A3FF28C0EF04FAC6D93452183F9

SHA1:	752BA98FA8471CC6C269BF9263A0335AB1C570D4
SHA256:	449149EABD216C3B638AFAE9AF82FEF24B69EDE7F6CD9060ED8D85C4F5C97D98
SSDEEP:	98304:dls3AMZYL//6sbANX5pm6UgyUuDQbeFUyk4ibBTpmmM2Q:X

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\Ficha_Tecnica_Juridica_N°_417394813..exe"	"C:\Users\admin\AppData\Local\Temp\Ficha_Tecnica_Juridica_N°_417394813..exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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