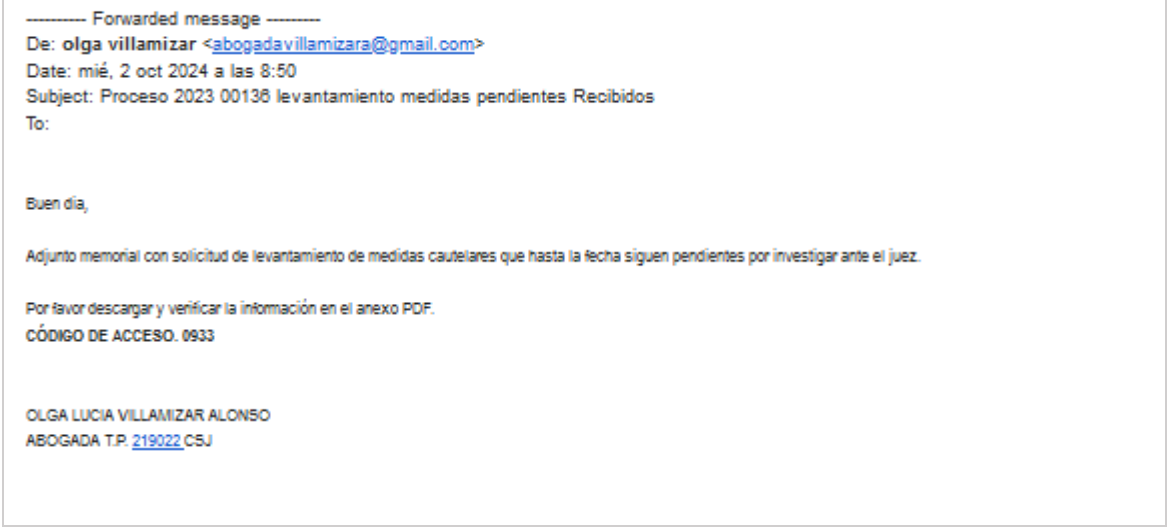
Octubre 06 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

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



---------- Forwarded message ---------
De: **olga villamizar** <abogadavillamizara@gmail.com>
Date: mié, 2 oct 2024 a las 8:50
Subject: Proceso 2023 00136 levantamiento medidas pendientes Recibidos
To:

Buen dia,

Adjunto memorial con solicitud de levantamiento de medidas cautelares que hasta la fecha siguen pendientes por investigar ante el juez.

Por favor descargar y verificar la información en el anexo PDF.
CÓDIGO DE ACCESO. 0933

OLGA LUCIA VILLAMIZAR ALONSO
ABOGADA T.P. 219022 CSJ

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:	Proceso 2023 00136 levantamiento medidas pendientes Recibidos.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	October 06, 2024 at 08:30:05
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	9e5634a01e241113ddc1a5a03265cd3e
SHA1:	17f3cba192f573754797b1fb6f644889f9abaaca
SHA256:	a8c0001bf62a178870fe526395703f682143078ad37d9b20e50f230dd9059648

SSDEEP:	49152:7lnKF46FKC9PgROSeQ146cDPM2vCVapdoqwicf1/y36sbwAE1JgZIESTcNY PMI3Y:7ld16SwwgZRbaEIo

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\<USER>\Desktop\PSE ACH No U867546753467890876545567897654345768907654 56.exe"	"C:\Users\<USER>\Desktop\PSE ACH No U867546753467890876545567897654345768907654 56.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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