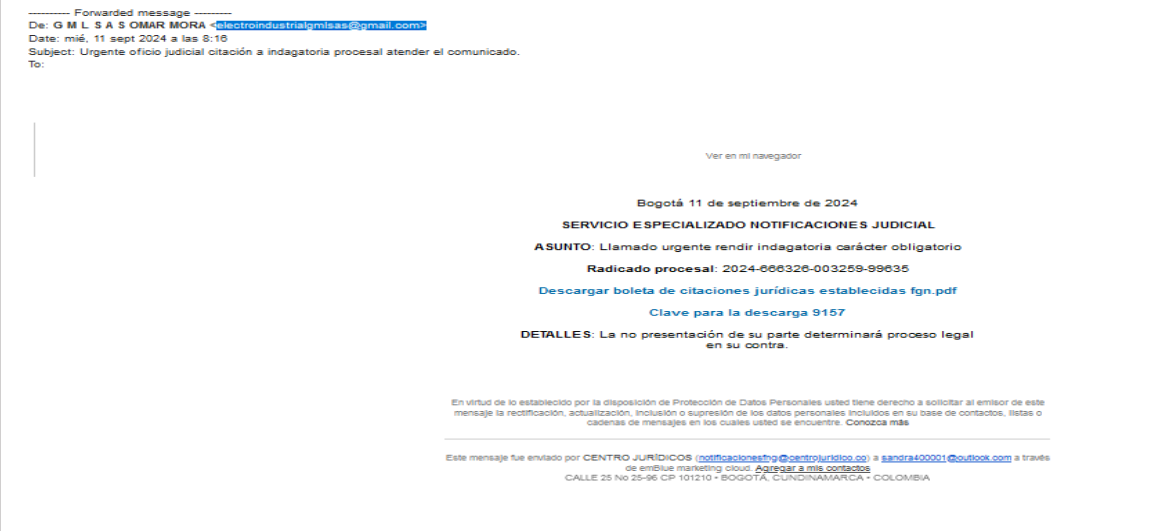
Septiembre 12 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.filerepmalware/misc
Cuenta de correo del remitente:	electroindustrialgmlsas@gmail.com
TLP:	**BLANCO**

Registro grafico relacionado con el Phishing



---------- Forwarded message ---------
De: G M L S A S OMAR MORA <electroindustrialgmlsas@gmail.com>
Date: mié, 11 sept 2024 a las 8:16
Subject: Urgente oficio judicial citación a indagatoria procesal atender el comunicado.
To:

Ver en mi navegador

Bogotá 11 de septiembre de 2024

SERVICIO ESPECIALIZADO NOTIFICACIONES JUDICIAL

ASUNTO: Llamado urgente rendir indagatoria carácter obligatorio

Radicado procesal: 2024-666326-003259-99635

Descargar boleta de citaciones jurídicas establecidas fgn.pdf

Clave para la descarga 9157

DETALLES: La no presentación de su parte determinará proceso legal en su contra.

En virtud de lo establecido por la disposición de Protección de Datos Personales usted tiene derecho a solicitar al emisor de este mensaje la rectificación, actualización, inclusión o supresión de los datos personales incluidos en su base de contactos, listas o cadenas de mensajes en los cuales usted se encuentre. Conozca más

Este mensaje fue enviado por CENTRO JURÍDICOS (notificacionesfng@centrojuridico.co) a sandra400001@outlook.com a través de emBlue marketing cloud. Agregar a mis contactos
CALLE 25 No 25-96 CP 101210 - BOGOTÁ, CUNDINAMARCA - 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:	DOCUMENTOS Y ANEXOS No 9876545789089765456758987657447567 89.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Septiembre 12, 2024 at 16:17:15
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	e066cbb0f6ac813bdbbfb52797d9b784

SHA1:	6c312b0f689b144451c3eec49d68d4da30e17218
SHA256:	4d144c8a4bfbbe489e042f996235c5afe0694f9a06f84abb3e50d6c3f64c7295
SSDEEP:	98304:G3x3FJ58yNV78P06chRcCOQhr6MSVV+uKIqKGx4rQ:G31H5nUKUCDzuKIqKKK

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\<USER>\Desktop\UMENTOS Y ANEXOS No 9876545789089765456758987657447567 89.exe"	"C:\Users\<USER>\Desktop\UMENTOS Y ANEXOS No 9876545789089765456758987657447567 89.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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