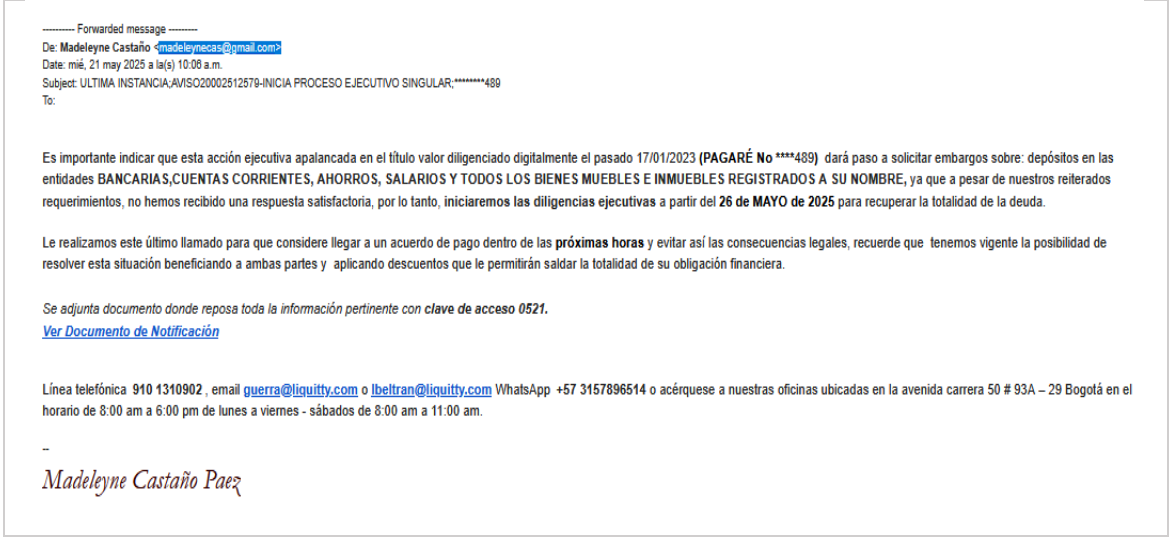
Mayo 21 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	downloader.
Cuenta de correo del remitente:	madeleynecas@gmail.com
TLP:	**BLANCO**

Registro grafico relacionado con el Phishing



---------- Forwarded message ---------
De: **Madeleyne Castaño** <madeleynecas@gmail.com>
Date: mié, 21 may 2025 a la(s) 10:08 a.m.
Subject: ULTIMA INSTANCIA;AVISO20002512579-INICIA PROCESO EJECUTIVO SINGULAR;********489
To:

Es importante indicar que esta acción ejecutiva apalancada en el título valor diligenciado digitalmente el pasado 17/01/2023 **(PAGARÉ No ****489)** dará paso a solicitar embargos sobre: depósitos en las entidades **BANCARIAS,CUENTAS CORRIENTES, AHORROS, SALARIOS Y TODOS LOS BIENES MUEBLES E INMUEBLES REGISTRADOS A SU NOMBRE,** ya que a pesar de nuestros reiterados requerimientos, no hemos recibido una respuesta satisfactoria, por lo tanto, **iniciaremos las diligencias ejecutivas** a partir del **26 de MAYO de 2025** para recuperar la totalidad de la deuda.

Le realizamos este último llamado para que considere llegar a un acuerdo de pago dentro de las **próximas horas** y evitar así las consecuencias legales, recuerde que tenemos vigente la posibilidad de resolver esta situación beneficiando a ambas partes y aplicando descuentos que le permitirán saldar la totalidad de su obligación financiera.

*Se adjunta documento donde reposa toda la información pertinente con **clave de acceso 0521.***
Ver Documento de Notificación

Línea telefónica **910 1310902** , email guerra@liquitty.com o lbeltran@liquitty.com WhatsApp **+57 3157896514** o acérquese a nuestras oficinas ubicadas en la avenida carrera 50 # 93A – 29 Bogotá en el horario de 8:00 am a 6:00 pm de lunes a viernes - sábados de 8:00 am a 11:00 am.

--
Madeleyne Castaño Paez

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:	EJCUTIVO SINGULA .489-20953-DGHED-34562-CVMFKD-5658-S2-452-423424-552D2-6-256-25626767-41.js
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	May 21, 2025 at 11:55:32
MIME:	text/plain
Información del archivo:	Unicode text, UTF-8 text, with very long lines (37320), with no line terminators
MD5:	7D7A6570445D009CC050EBCD2C435BA7
SHA1:	8A6785E6BCCF14C0FDEC47A14CE3AAD7CC9059C1

SHA256:	06324AD0F395C908EC2D9A7D8B59F7F026BADB34F6284EE6A0DB9C010A19E53A
SSDEEP:	768:HX99e79JfS++qMFFqP5+jgjjFuFltdH3q4KF/f+omaf:HXiWc

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Windows\System32\WScript.exe" "C:\Users\admin\AppData\Local\Temp\EJCUTIVO SINGULA .489-20953-DGHED-34562-CVMFKD-5658-S2-452-423424-552D2-6-256-25626767-41.js"	"C:\Windows\System32\WScript.exe" "C:\Users\admin\AppData\Local\Temp\EJCUTIVO SINGULA .489-20953-DGHED-34562-CVMFKD-5658-S2-452-423424-552D2-6-256-25626767-41.js"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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