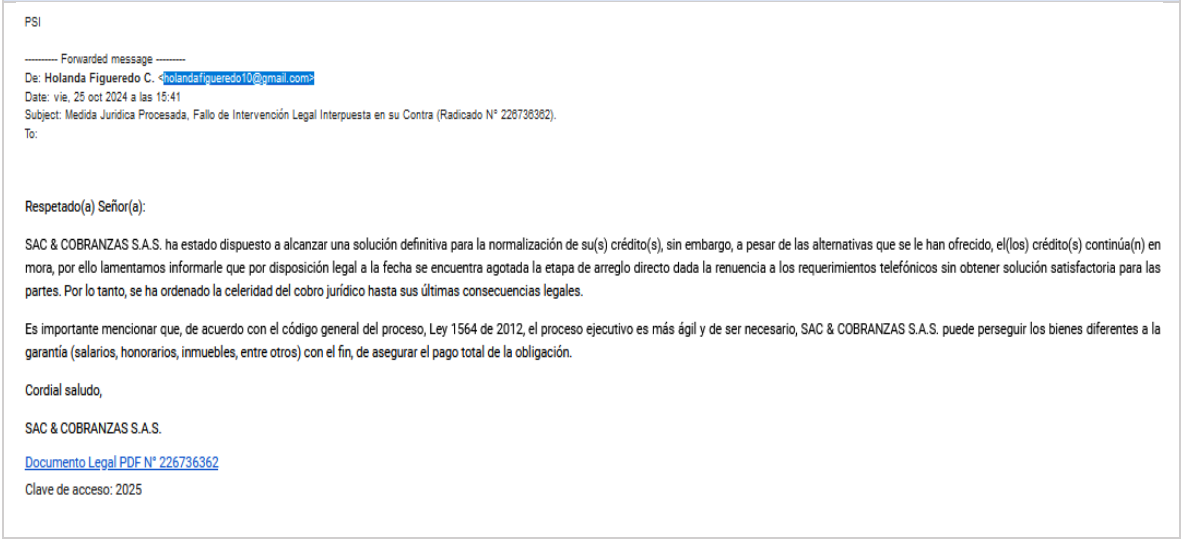
Octubre 28 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.filerepmalware
Cuenta de correo del remitente:	holandafigueredo10@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



PSI

---------- Forwarded message ---------
De: **Holanda Figueredo C.** <holandafigueredo10@gmail.com>
Date: vie, 25 oct 2024 a las 15:41
Subject: Medida Juridica Procesada, Fallo de Intervención Legal Interpuesta en su Contra (Radicado N° 226736362).
To:

Respetado(a) Señor(a):

SAC & COBRANZAS S.A.S. ha estado dispuesto a alcanzar una solución definitiva para la normalización de su(s) crédito(s), sin embargo, a pesar de las alternativas que se le han ofrecido, el(los) crédito(s) continúa(n) en mora, por ello lamentamos informarle que por disposición legal a la fecha se encuentra agotada la etapa de arreglo directo dada la renuencia a los requerimientos telefónicos sin obtener solución satisfactoria para las partes. Por lo tanto, se ha ordenado la celeridad del cobro jurídico hasta sus últimas consecuencias legales.

Es importante mencionar que, de acuerdo con el código general del proceso, Ley 1564 de 2012, el proceso ejecutivo es más ágil y de ser necesario, SAC & COBRANZAS S.A.S. puede perseguir los bienes diferentes a la garantía (salarios, honorarios, inmuebles, entre otros) con el fin, de asegurar el pago total de la obligación.

Cordial saludo,

SAC & COBRANZAS S.A.S.

Documento Legal PDF N° 226736362

Clave de acceso: 2025

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:	Radicado_Legal.N°93883..exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	October 28, 2024 at 10:21:50
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows, 10 sections
MD5:	81225DDA9225995E9C584C9984119238

SHA1:	7F468D190E9A34DB1357BDBE19911C0A8D427D3C
SHA256:	495897A0E9D55BBD06884DF8B9B7C15D9C398E825538D7A235CBFB7D75D4B99E
SSDEEP:	49152:er3k/ulwZAGy0AJ/+ZTdBRAG/HzXCdNmSxDMNr2NqhZPHLIbwqiMVVeva+aRIx3Y:f/utGyp/DMQQh6otGIPnqNb

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\Radicado_Legal.N°93883..exe"	"C:\Users\admin\AppData\Local\Temp\Radicado_Legal.N°93883..exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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