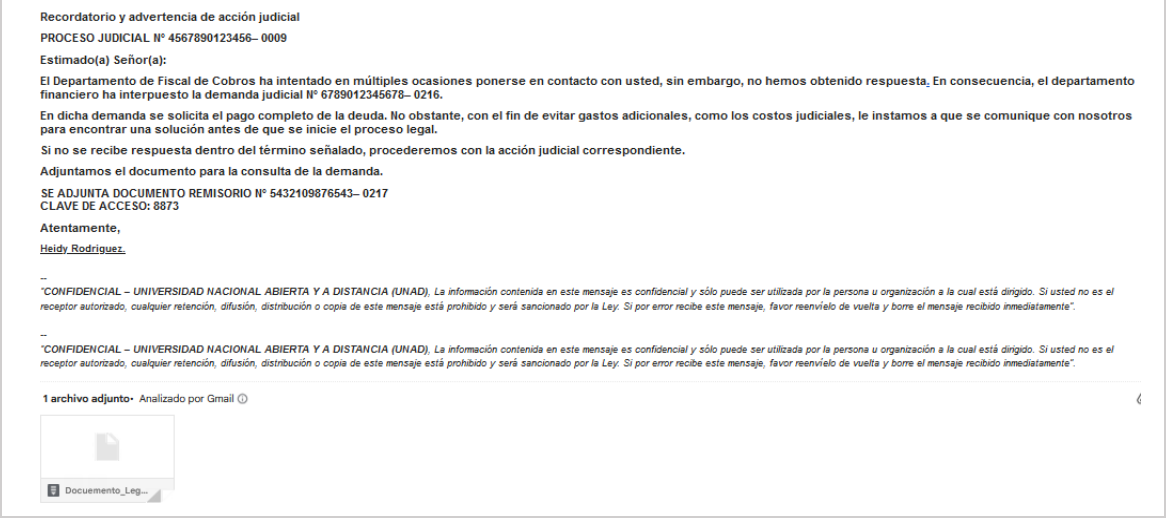
Enero 23 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

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



Recordatorio y advertencia de acción judicial

PROCESO JUDICIAL N° 4567890123456– 0009

Estimado(a) Señor(a):

El Departamento de Fiscal de Cobros ha intentado en múltiples ocasiones ponerse en contacto con usted, sin embargo, no hemos obtenido respuesta. En consecuencia, el departamento financiero ha interpuesto la demanda judicial N° 6789012345678– 0216.

En dicha demanda se solicita el pago completo de la deuda. No obstante, con el fin de evitar gastos adicionales, como los costos judiciales, le instamos a que se comunique con nosotros para encontrar una solución antes de que se inicie el proceso legal.

Si no se recibe respuesta dentro del término señalado, procederemos con la acción judicial correspondiente.

Adjuntamos el documento para la consulta de la demanda.

SE ADJUNTA DOCUMENTO REMISORIO N° 5432109876543– 0217
CLAVE DE ACCESO: 8873

Atentamente,

Heidy Rodriguez.

--
"CONFIDENCIAL – UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD), La información contenida en este mensaje es confidencial y sólo puede ser utilizada por la persona u organización a la cual está dirigido. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje está prohibido y será sancionado por la Ley. Si por error recibe este mensaje, favor reenvíelo de vuelta y borre el mensaje recibido inmediatamente".

--
"CONFIDENCIAL – UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD), La información contenida en este mensaje es confidencial y sólo puede ser utilizada por la persona u organización a la cual está dirigido. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje está prohibido y será sancionado por la Ley. Si por error recibe este mensaje, favor reenvíelo de vuelta y borre el mensaje recibido inmediatamente".

1 archivo adjunto· Analizado por Gmail

Docuemento_Leg...

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:	Docuemento_Legal.N°00182812-8873.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	January 23, 2025 at 13:32:45
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows, 6 sections
MD5:	45A6E7FE6D7E833F374DABE4A3E08BA3
SHA1:	77CD883B68F9C678C3B3228958D1170755147AC6
SHA256:	AD5A5FD9F54B29D1BB9F6A9E6915CF059E1560B68F493323BA77BF3FB5A12C12

SSDEEP:	98304:cjkqYS00AnJ/LCduUdbWo2F7tVQq4IzGUNp2y:

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\Docue mento Legal.N°00182812-8873.exe"	"C:\Users\admin\AppData\Local\Temp\Docue mento Legal.N°00182812-8873.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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