Enero 16 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.gatak/obudo
Cuenta de correo del remitente:	auxcontable@munozcargo.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	

---------- Forwarded message ----------
De: **auxcontable** <auxcontable@munozcargo.com>
Date: mar, 14 ene 2025 a las 20:57
Subject: Notificación de Acción Ejecutiva_459873052922422
To: <sthumano@unad.edu.co>

JUZGADO SEGUNDO CIVIL MUNICIPAL DE BOGOTÁ

Carrera 17 No. 42-70, Edificio Justicia

Bogotá, Colombia

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

Cc / Nit: 8605127804

Estimado/a

sthumano@unad.edu.co

Por medio de la presente, le informamos que se ha iniciado un proceso judicial en el Juzgado Segundo Civil Municipal de Bogotá, con el radicado 2024-102744, relacionado con la deuda pendiente a su cargo.

En este sentido, adjuntamos los documentos pertinentes, los cuales deben ser validados mediante firma electrónica. Para ello, le solicitamos seguir los pasos a continuación:

1. Descargue los archivos en formatos PDF.
2. Detalles_Judiciales_Adjuntos_Descargue
3. Utilice la clave **14325** para acceder y validar los documentos.

El plazo máximo de tres (3) días hábiles contados a partir de la recepción de esta notificación, En caso de no realizar el pago dentro del plazo estipulado, procederemos a tomar las acciones legales correspondientes.

Atentamente,
Maria Fernanda Lopez Rodriguez
Juzgado Segundo Civil Municipal de Bogotá

Nota: Este es un mensaje automatizado. No responda a este correo.

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:	ad923417508192740683541275809327612498561092384765 01(1).exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	January 16, 2025 at 14:26:38

MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows, 8 sections
MD5:	E2909CE9F9ACF027481CBA55C71F8253
SHA1:	D01DBF511D63C4743467BC9A7415477AC60CC6B5
SHA256:	DA32159B27065337A699264DA4778B7C99F8FBB4F00617061B9A5B5397BD5973
SSDEEP:	49152:9H7l8iF+nFy8rFZunc5gJB2IshaU+KvuwpiLqprQ2wQ1QxPtXSQA37jdbMwZIAyi:VNIFy8rFZB5gKjhabKvuwpiOt309vAL3

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\ad9234175081927406835412758093276124985610923847650 1(1).exe"	"C:\Users\admin\AppData\Local\Temp\ad9234175081927406835412758093276124985610923847650 1(1).exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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