Abril 05 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.dffcd/minerva
Cuenta de correo del remitente:	personeria@launion-antioquia.gov.co
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	

---------- Forwarded message ---------
De: **personeria launion-antioquia** <personeria@launion-antioquia.gov.co>
Date: jue, 3 abr 2025 a la(s) 9:35 a.m.
Subject: ACCIONAR JUDICIAL - INSTAURACION DE TUTELA
To:

JUZGADO PROMISCUO MUNICIPAL
SALA DISCIPLINARIA DE ACCIÓN JUDICIAL

Cordial saludo,

De manera atenta y precisa se emite la tutela instaurada en la fecha 03-04-2025 por los hechos que a continuación se presentan dentro del archivo adjunto
Por lo anterior solicitamos verificar la información dentro del archivo adjunto

VER AQUÍ O DESCARGAR ARCHIVO ADJUNTO AL FINAL DE DOCUMENTO
CÓDIGO DE ACCESO 0944

RAMA JUDICIAL
DIRECCIÓN EJECUTIVA DE
ADMINISTRACIÓN JUDICIAL

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:	ACCIONAR TUTELA 0944.bat
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	April 05, 2025 at 10:26:01
MIME:	text/plain
Información del archivo:	ASCII text, with very long lines (60231), with CRLF, LF line terminators
MD5:	116B68093C55FFBA843DEACA29A98FFC
SHA1:	3E7FBC9772E5D0989FFFD0D1A3610AFE267D8796

SHA256:	23A778FF353A75880CC93B92A1503F005FDD26CBBE6D4175C42F5C5EA42FDA64
SSDEEP:	6144:4XW1Ck9zyf+rDimRxD3cn3n32BCCU91TP+pmAB+x4yzAzRK1lkKf9qigy:wk5FCmRpS2BsymABdRKLkKfsiD

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
C:\WINDOWS\system32\cmd.exe /c ""C:\Users\admin\AppData\Local\Temp\ACCIONAR TUTELA 0944.bat" "	C:\WINDOWS\system32\cmd.exe /c ""C:\Users\admin\AppData\Local\Temp\ACCIONAR TUTELA 0944.bat" "	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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