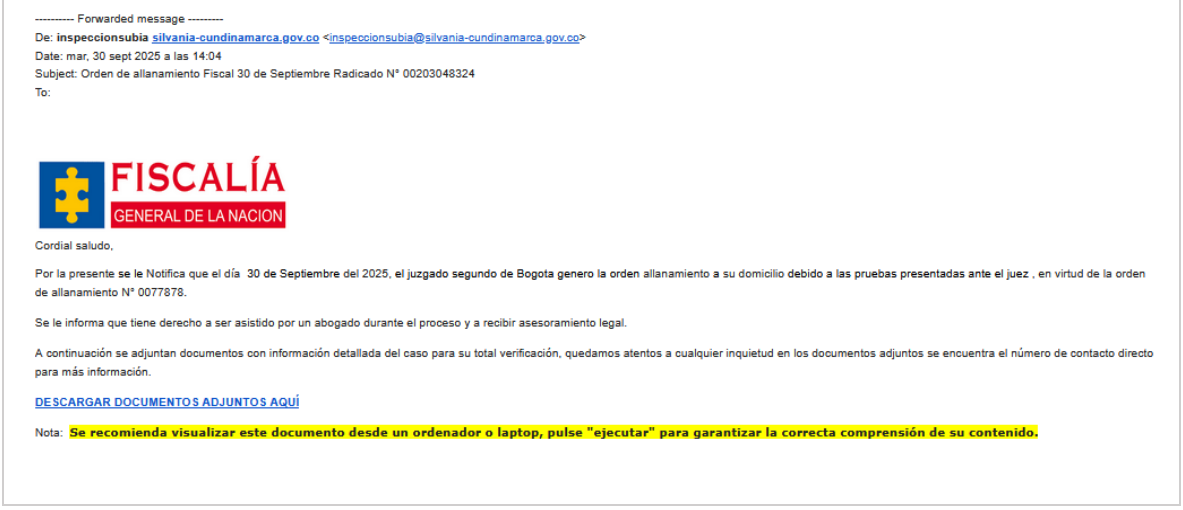
Octubre 01 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	UDS:Trojan-Downloader.WinINF.Seraph.gen
Cuenta de correo del remitente:	inspeccionsubia@silvania-cundinamarca.gov.co
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ---------
De: **inspeccionsubia** silvania-cundinamarca.gov.co <inspeccionsubia@silvania-cundinamarca.gov.co>
Date: mar, 30 sept 2025 a las 14:04
Subject: Orden de allanamiento Fiscal 30 de Septiembre Radicado N° 00203048324
To:

FISCALÍA GENERAL DE LA NACION

Cordial saludo,

Por la presente se le Notifica que el día 30 de Septiembre del 2025, el juzgado segundo de Bogota genero la orden allanamiento a su domicilio debido a las pruebas presentadas ante el juez , en virtud de la orden de allanamiento N° 0077878.

Se le informa que tiene derecho a ser asistido por un abogado durante el proceso y a recibir asesoramiento legal.

A continuación se adjuntan documentos con información detallada del caso para su total verificación, quedamos atentos a cualquier inquietud en los documentos adjuntos se encuentra el número de contacto directo para más información.

DESCARGAR DOCUMENTOS ADJUNTOS AQUÍ

Nota: **Se recomienda visualizar este documento desde un ordenador o laptop, pulse "ejecutar" para garantizar la correcta comprensión de su contenido.**

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:	Documento de allanamiento Fiscal 30 de Septiembre Radicado N° 00203048324.url
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	October 01, 2025 at 12:46:32
MIME:	application/x-wine-extension-ini
Información del archivo:	Generic INItialization configuration [InternetShortcut]
MD5:	CA4B1FE560AEE2C2E01781EE2495FDA2
SHA1:	81F36B15F94960B5D7AFD82FEA29408690608FAB

SHA256:	DE541A634C6FF601CD4DE42D29841928BB344FB15392056F9C615BB6033104A5
SSDEEP:	6:JyXSvVG/FTVmJtOFJb5if5oeTckmrISDX/sxsv:cXaVWfmJtOFJQRzgrDX/so

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\WINDOWS\system32\rundll32.exe" "C:\WINDOWS\system32\ieframe.dll",OpenURL %l	"C:\WINDOWS\system32\rundll32.exe" "C:\WINDOWS\system32\ieframe.dll",OpenURL %l	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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