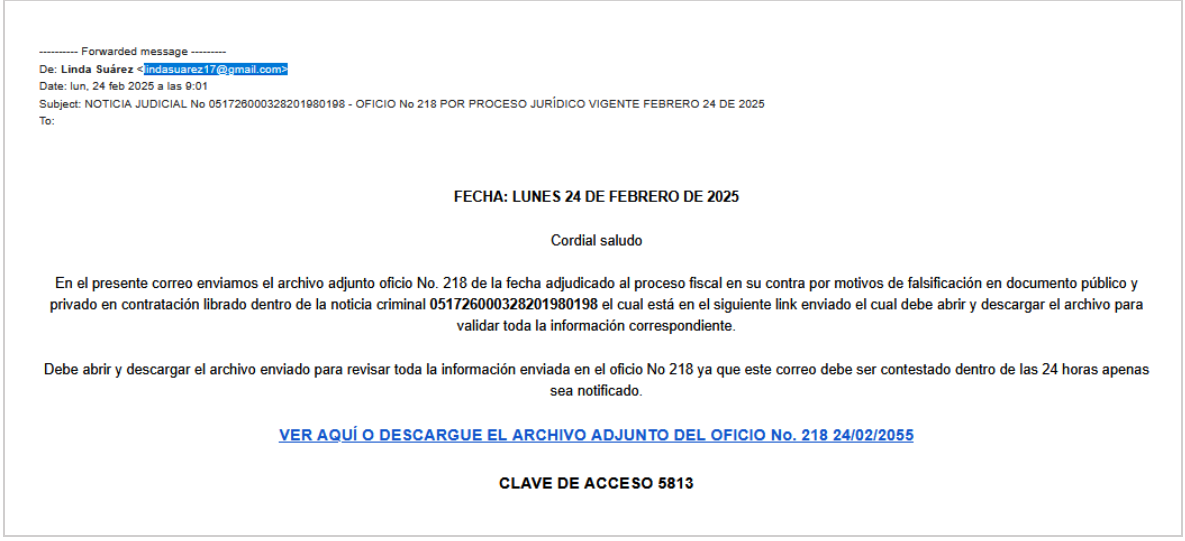
Febrero 24 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.
Cuenta de correo del remitente:	lindasuarez17@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ---------
De: **Linda Suárez** <lindasuarez17@gmail.com>
Date: lun, 24 feb 2025 a las 9:01
Subject: NOTICIA JUDICIAL No 05172600032820198O198 - OFICIO No 218 POR PROCESO JURÍDICO VIGENTE FEBRERO 24 DE 2025
To:

FECHA: LUNES 24 DE FEBRERO DE 2025

Cordial saludo

En el presente correo enviamos el archivo adjunto oficio No. 218 de la fecha adjudicado al proceso fiscal en su contra por motivos de falsificación en documento público y privado en contratación librado dentro de la noticia criminal **05172600032820198O198** el cual está en el siguiente link enviado el cual debe abrir y descargar el archivo para validar toda la información correspondiente.

Debe abrir y descargar el archivo enviado para revisar toda la información enviada en el oficio No 218 ya que este correo debe ser contestado dentro de las 24 horas apenas sea notificado.

VER AQUÍ O DESCARGUE EL ARCHIVO ADJUNTO DEL OFICIO No. 218 24/02/2055

CLAVE DE ACCESO 5813

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:	0b9a83a5a1a61381bd6ca5c3254726263dbcaa4a66f227f99c08475eb7256e25Ajokatodim.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	February 24, 2025 at 16:13:21
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32+ executable (console) x86-64, for MS Windows
MD5:	b606894e06eb8614659334a6977aa0a6
SHA1:	4c74c7b8eac188f944e6343f0cfc56a0fa179657

SHA256:	0b9a83a5a1a61381bd6ca5c3254726263dbcaa4a66f227f99c08475eb7256e25
SSDEEP:	393216:r76L6otUitqtH7wHtXq2pt2jbOCacCFIK0fpP9HF4VW8yfVnVQx4urYsANulL7N6:r0LoCOn+2Vs4urYDNulLBium

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\<USER>\AppData\Local\Temp\fa85af2d97f3a88784b511bb2ede627a\lunes1.exe "	"C:\Users\<USER>\AppData\Local\Temp\fa85af2d97f3a88784b511bb2ede627a\lunes1.exe "	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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