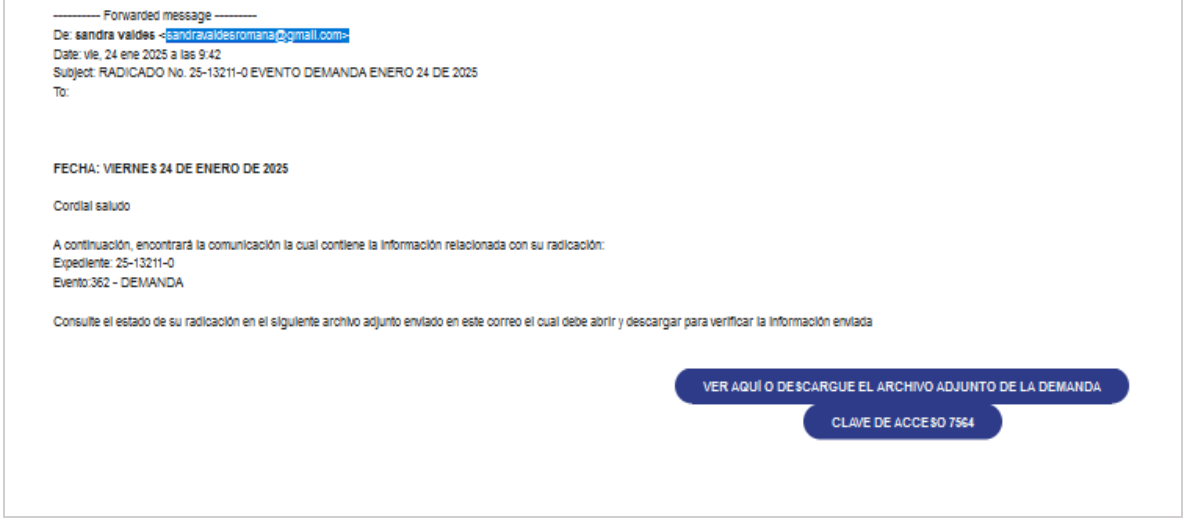
Enero 24 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

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



---------- Forwarded message ---------
De: sandra valdes <sandravaldesromana@gmail.com>
Date: vie, 24 ene 2025 a las 9:42
Subject: RADICADO No. 25-13211-0 EVENTO DEMANDA ENERO 24 DE 2025
To:

FECHA: VIERNES 24 DE ENERO DE 2025

Cordial saludo

A continuación, encontrará la comunicación la cual contiene la información relacionada con su radicación:
Expediente: 25-13211-0
Evento:362 - DEMANDA

Consulte el estado de su radicación en el siguiente archivo adjunto enviado en este correo el cual debe abrir y descargar para verificar la información enviada

VER AQUÍ O DESCARGUE EL ARCHIVO ADJUNTO DE LA DEMANDA

CLAVE DE ACCESO 7564

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:	RADICADO No. 25-13211-0 EVENTO DEMANDA ENERO 24 DE 2025.vbs
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	January 24, 2025 at 10:23:54
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows, 6 sections
MD5:	674D1335A8625B6C37C395311BCC3E82
SHA1:	0FE3A99645AA468FA2104A8E2FBFF79137B1FA35
SHA256:	D6E616298227E42BD5B3C41F6213C8F8BB05DF6994195C40D949ABC42A5F5103

SSDEEP:	3072:h5LVmI3b0mgfmWu+ye9VOv5iG5sVhQ30Wk+70wgA11:h5LV7e9VOvp

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\WINDOWS\System32\OpenWith.exe" "C:\Users\admin\AppData\Local\Temp\RADICADO No. 25-13211-0 EVENTO DEMANDA ENERO 24 DE 2025.vbs.vba"	"C:\WINDOWS\System32\OpenWith.exe" "C:\Users\admin\AppData\Local\Temp\RADICADO No. 25-13211-0 EVENTO DEMANDA ENERO 24 DE 2025.vbs.vba"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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