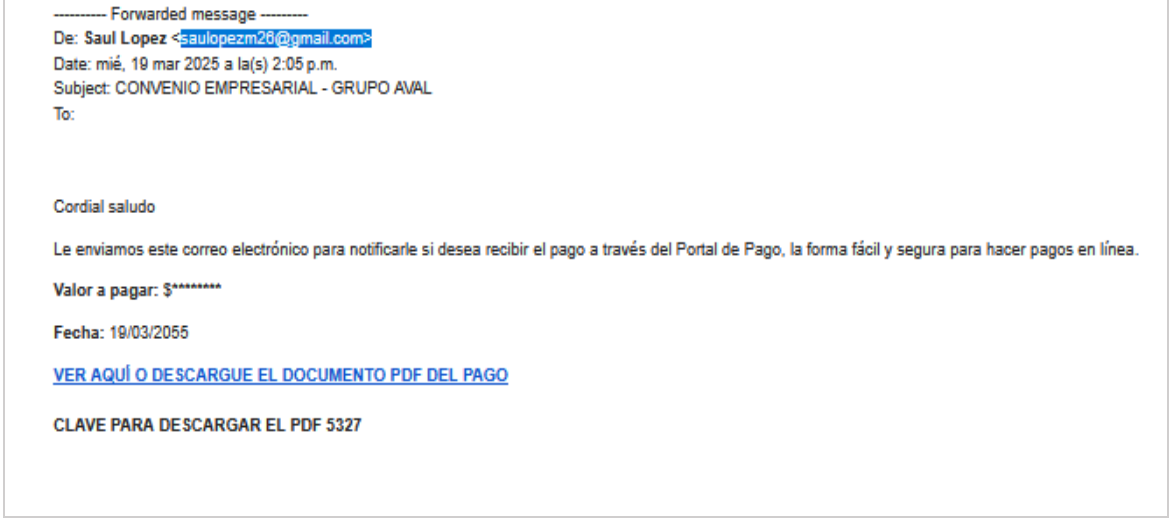
Marzo 20 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.
Cuenta de correo del remitente:	saulopezm26@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ---------
De: **Saul Lopez** <saulopezm26@gmail.com>
Date: mié, 19 mar 2025 a la(s) 2:05 p.m.
Subject: CONVENIO EMPRESARIAL - GRUPO AVAL
To:

Cordial saludo

Le enviamos este correo electrónico para notificarle si desea recibir el pago a través del Portal de Pago, la forma fácil y segura para hacer pagos en línea.

Valor a pagar: $*********

Fecha: 19/03/2055

VER AQUÍ O DESCARGUE EL DOCUMENTO PDF DEL PAGO

CLAVE PARA DESCARGAR EL PDF 5327

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:	ACUERDO DE TRANSACCIÓN FINANCIERA ACH ; 6897854.bat
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	March 20, 2025 at 10:54:37
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows, 11 sections
MD5:	6c9aea828edbb3bc0d10a917936963b4
SHA1:	698c82d4ce931f7db9d16b8b1198ee6d4f082773

SHA256:	9bc2a757994f0f865120d7b4734fd181556271fb15685235e58ef5b6acadf2ce
SSDEEP:	1536:4JmXGmXQepX+TREsbKGwamzZkbmEKUgXEXzICKUnFsv:4c2fepK5W0m+Hf+

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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