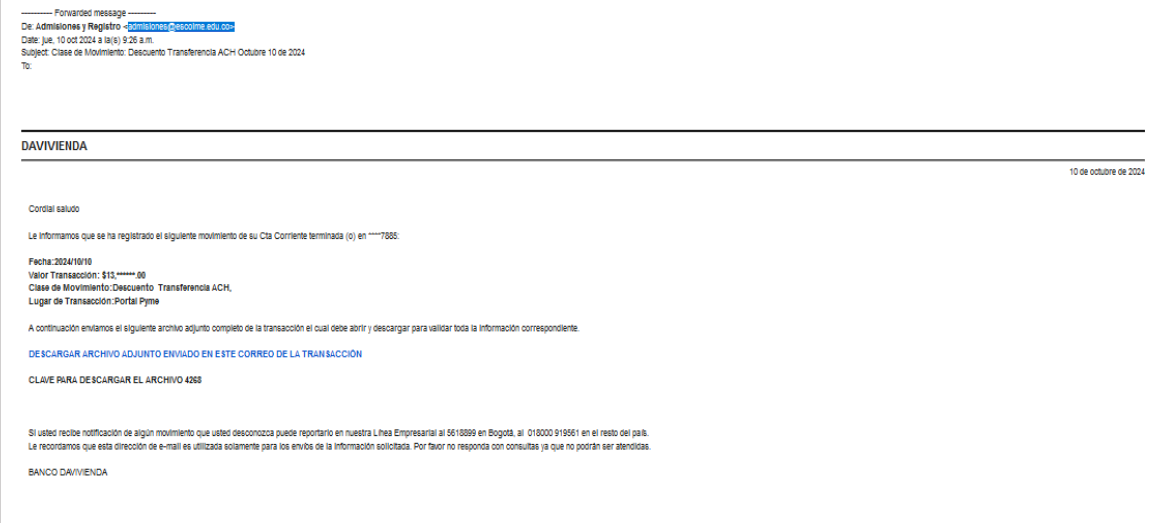
Octubre 11 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.filerepmalware/hcpn
Cuenta de correo del remitente:	admisiones@escolme.edu.co
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ---------
De: **Admisiones y Registro** <admisiones@escolme.edu.co>
Date: jue, 10 oct 2024 a la(s) 9:26 a.m.
Subject: Clase de Movimiento: Descuento Transferencia ACH Octubre 10 de 2024
To:

DAVIVIENDA

10 de octubre de 2024

Cordial saludo

Le informamos que se ha registrado el siguiente movimiento de su Cta Corriente terminada (o) en ****7886:

Fecha:2024/10/10
Valor Transacción: $13,****.00**
Clase de Movimiento:Descuento Transferencia ACH,
Lugar de Transacción:Portal Pyme

A continuación enviamos el siguiente archivo adjunto completo de la transacción el cual debe abrir y descargar para validar toda la información correspondiente.

DESCARGAR ARCHIVO ADJUNTO ENVIADO EN ESTE CORREO DE LA TRANSACCIÓN

CLAVE PARA DESCARGAR EL ARCHIVO 4268

Si usted recibe notificación de algún movimiento que usted desconozca puede reportarlo en nuestra Línea Empresarial al 5618899 en Bogotá, al 018000 919561 en el resto del país.
Le recordamos que esta dirección de e-mail es utilizada solamente para los envíos de la información solicitada. Por favor no responda con consultas ya que no podrán ser atendidas.

BANCO DAVIVIENDA

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:	TRANSFERENCIA ACH NO 98768574565879097658746578 9.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	October 11, 2024 at 13:54:56
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	FB652B5FF3A97EBBB8C9BF69C7010C1C
SHA1:	49ACDEB895D801DD4439FAD35337B19BACA56D65
SHA256:	4D37F7AEA76CCB788710E7D3A8D2553964142A835115A9F0768F33B286400352

SSDEEP:	98304:8l1IlkppkPcoCjEWOJ2PfANSkH6hxb7zQgmOL1i2GkSBA3Gn1OM4lzgsUGoxkrgx:Ew4ax

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\TRANSFERENCIA ACH NO 98768574565879097658746578 9.exe"	"C:\Users\admin\AppData\Local\Temp\TRANSFERENCIA ACH NO 98768574565879097658746578 9.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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