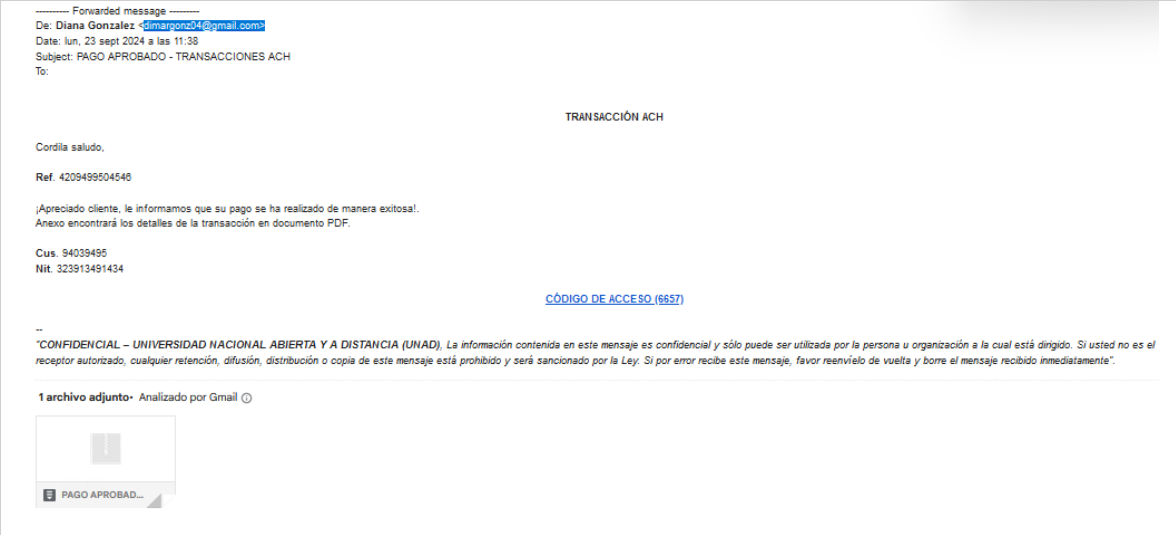
Septiembre 23 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.lazy/filerepmalware
Cuenta de correo del remitente:	dimargonz04@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	


---------- Forwarded message ---------
De: **Diana Gonzalez** <dimargonz04@gmail.com>
Date: lun, 23 sept 2024 a las 11:38
Subject: PAGO APROBADO - TRANSACCIONES ACH
To:

TRANSACCIÓN ACH

Cordila saludo,

Ref. 4209499504546

¡Apreciado cliente, le informamos que su pago se ha realizado de manera exitosa!.
Anexo encontrará los detalles de la transacción en documento PDF.

Cus. 94039495
Nit. 323913491434

CÓDIGO DE ACCESO (6657)

--
"CONFIDENCIAL – UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD), La información contenida en este mensaje es confidencial y sólo puede ser utilizada por la persona u organización a la cual está dirigido. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje está prohibido y será sancionado por la Ley. Si por error recibe este mensaje, favor reenvíelo de vuelta y borre el mensaje recibido inmediatamente".

1 archivo adjunto• Analizado por Gmail

PAGO APROBAD...

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:	PAGO APROBADO - TRANSACCIONES ACH.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Septiembre 23, 2024 at 16:13:30
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	515DB4F6275767476E5694ACECF9CBEB

SHA1:	3D4E8845DE05195402F8E3E13B8F6F7833868927
SHA256:	72DF2AEC1FFC4AA6B345C79159BA506CE4BBC0DFE9E0FF15B7CC1EDE56BAC281
SSDEEP:	98304:+9Vvg0eyFOTC+r0qYbFwmCmqIuhY62CLhXJFztsHiIN:+

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\PAGO APROBADO - TRANSACCIONES ACH.exe"	"C:\Users\admin\AppData\Local\Temp\PAGO APROBADO - TRANSACCIONES ACH.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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