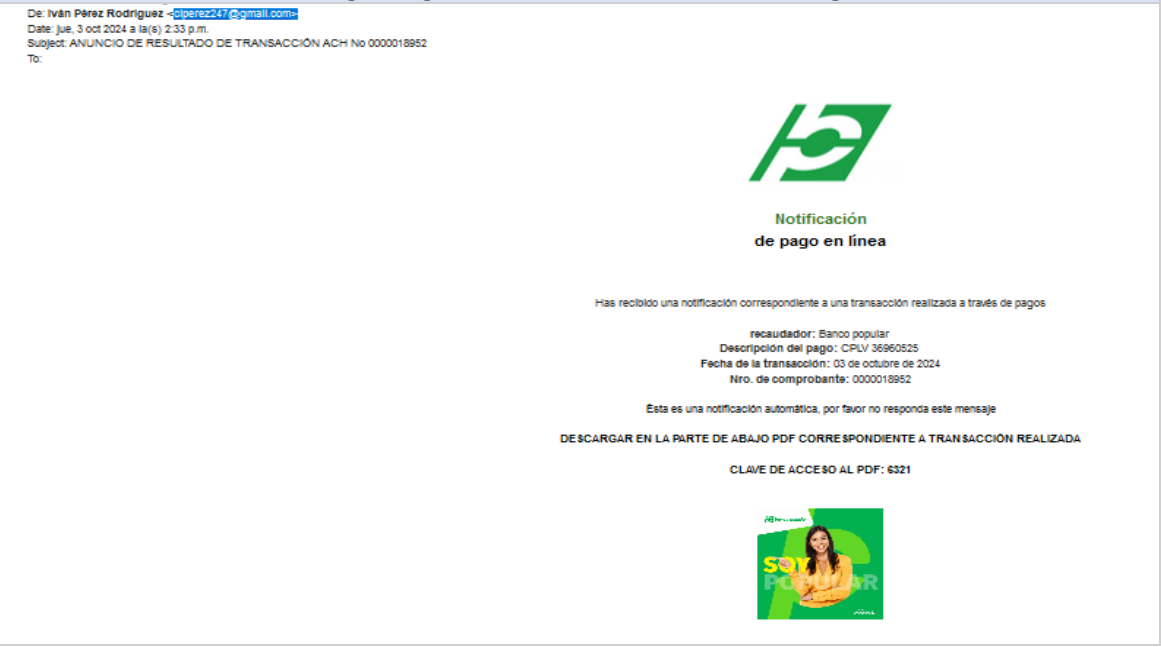
Octubre 03 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.filerepmalware
Cuenta de correo del remitente:	ciperez247@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	


De: Iván Pérez Rodriguez <ciperez247@gmail.com>
Date: jue, 3 oct 2024 a la(s) 2:33 p.m.
Subject: ANUNCIO DE RESULTADO DE TRANSACCIÓN ACH No 0000018952
To:

Notificación
de pago en línea

Has recibido una notificación correspondiente a una transacción realizada a través de pagos

recaudador: Banco popular
Descripción del pago: CPLV 36960525
Fecha de la transacción: 03 de octubre de 2024
Nro. de comprobante: 0000018952

Esta es una notificación automática, por favor no responda este mensaje

DESCARGAR EN LA PARTE DE ABAJO PDF CORRESPONDIENTE A TRANSACCIÓN REALIZADA

CLAVE DE ACCESO AL PDF: 6321

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:	ANUNCIO DE RESULTADO DE TRANSACCIÓN ACH No 0000018952.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	October 03, 2024 at 16:32:22
MIME:	application/x-dosexec

Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	BC7C2B5CECB62DDDA8AB33EAAA7ABF65
SHA1:	E8EA016E57A0E87B90F8AFBCE0EEE6BC1AFD8BFB
SHA256:	0E875809AFEC874BBBDD8395EFAC33C3E57BD86A66AE4097C87B35656B64804C
SSDEEP:	49152:wIOYx1uI7XDDYt3L5u9r9p9RSS7UT1xzWdGkM4feuO8+m3evARXXky37Y2zB9GJ2:rbuI73YtqUJd8+mlokA1eiAvkRum/y+y

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\ANUNCIO DE RESULTADO DE TRANSACCIÓN ACH No 0000018952.exe"	"C:\Users\admin\AppData\Local\Temp\ANUNCIO DE RESULTADO DE TRANSACCIÓN ACH No 0000018952.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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