Enero 29 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

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

---------- Forwarded message ---------
De: **TUMI S.A.S** <tumisasgestiondecartera@gmail.com>
Date: mié, 29 ene 2025 a la(s) 11:48 a.m.
Subject: DAVIVIENDA - CÁRTER FINANCIERA REF. N ° 0939495954
To:

DAVIVIENDA

SOPORTE DE TRANSACCIÓN

Cordial saludo

Le informamos que el pago generado desde portales bancarios se ha realizado de manera exitosa!

Anexo encontrará los detalles de la transacción.
Le solicitamos verificar la información dentro del archivo adjunto

Estado de transacción. Realizada
N° ref. 0939495954

VER AQUÍ O DESCARGAR ARCHIVO ADJUNTO AL FINAL DE DOCUMENTO
CÓDIGO DE ACCESO 8845

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:	DAVIVIENDA - CÁRTER FINANCIERA REF. N ° 0939495954.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	January 29, 2025 at 12:12:43
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows, 7 sections
MD5:	BE9070CEF329332F8AFA74C091D2EF15
SHA1:	D1D836E7885404D6986E39907C361F3EEDB76B5A
SHA256:	9F5A7D655C1227E0EA7E7409D1AAEFB956D3655C6125B757FC000E3EBA8B8EA0

SSDEEP:	98304:QbR4IureGNwDs9FACqUEQNHN16ZpWV98q8nq1BheQVnGVkM/90oXbxdffA:

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\DAVIVIENDA - CÁRTER FINANCIERA REF. N ° 0939495954.exe"	"C:\Users\admin\AppData\Local\Temp\DAVIVIENDA - CÁRTER FINANCIERA REF. N ° 0939495954.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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