Noviembre 07 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.remcos/vpxnb
Cuenta de correo del remitente:	fasolem.23@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	

--------- Forwarded message ---------
De: **FAMILIAS SOLIDARIAS EMPRENDEDORAS** <fasolem.23@gmail.com>
Date: mar, 5 nov 2024 a las 13:05
Subject: Fwd: Aviso de Regularización de Multas de Tránsito – Radicado N° 65225-56612-2024-200332
To:

ARCHIVO ADJUNTO - PDF PROTEGIDO CLAVE 202410 - VISUALIZAR EL DOCUMENTO EN UN ORDENADOR O LAPTOP

Asunto: Aviso de Regularización de Multas de Tránsito – Radicado N° 65225-56612-2024-200332

De: Agencia de Tránsito y Transporte.
Fecha: 05 de octubre de 2024

Estimado/a :

En calidad de **Agencia de Tránsito y Transporte**, le informamos que, de acuerdo con el **Radicado N° 65225-56612-2024-200332**, todos los conductores de vehículos y motocicletas con multas pendientes deben **ponerse al día** con sus obligaciones antes del **06 de noviembre de 2024**, a fin de evitar recargos adicionales por intereses por morosidad.

Se recomienda visualizar este documento desde un ordenador o laptop para garantizar la correcta comprensión de su contenido.

Recuerde que las multas pendientes generan intereses que aumentan con el tiempo. Puede realizar el pago a través de nuestros canales habilitados.

Para más información, puede contactar a nuestra oficina o consultar en línea.

ARCHIVO ADJUNTO - PDF PROTEGIDO CLAVE 202410 - VISUALIZAR EL DOCUMENTO EN UN ORDENADOR O LAPTOP

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:	Recuerde que las multas pendientes generan intereses que aumentan con el tiempo. Puede realizar el pago a través de nuestros canales habilitados..exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	November 07, 2024 at 15:43:40
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows, 3 sections
MD5:	ED0AE38627419BD16B2DBD7154116843
SHA1:	97933C544939E4C1BFCD336AF374CDFEBE1D529B

SHA256:	D0E1E79266C3E2428E10998EFA4E55B571F7C21A02DFD18C6BFB560D1DB919B6
SSDEEP:	98304:pyz+2tFRAyQncHK9Rykw9iDMwoPy+cljQziHRL/9OSXnVtJwVPXVuD43qK8TuupN:czV

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\f331ae4a-1e79-4e4e-ae58-4c64a5c449a1.exe"	"C:\Users\admin\AppData\Local\Temp\f331ae4a-1e79-4e4e-ae58-4c64a5c449a1.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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