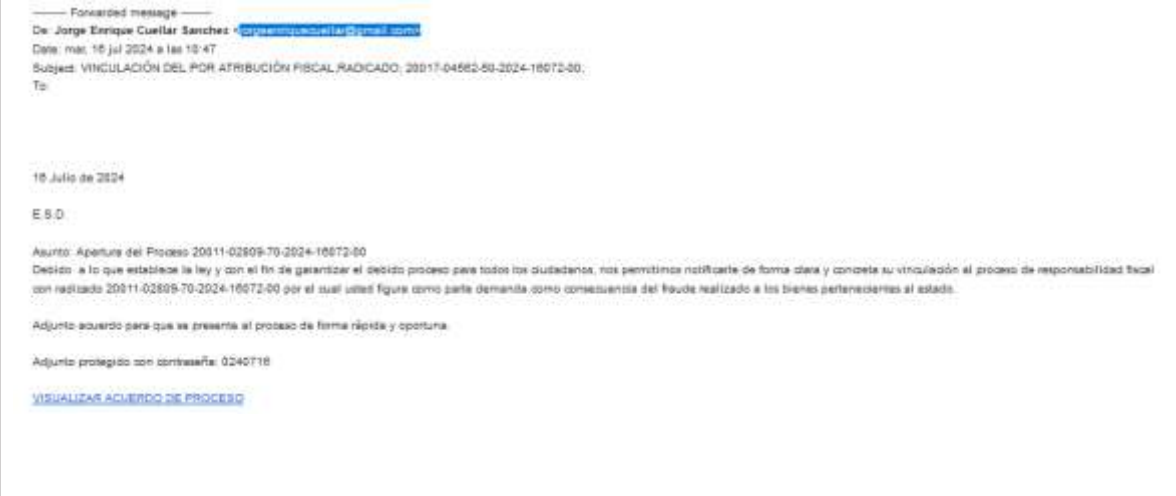
Julio 16 de 2024

**COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING**

| | |
|---|---|
| **Técnica Mitre**: | Phishing |
| **Malware detectado**: | trojan.androm/msil |
| **Cuenta de correo del remitente:** | jorgeenriquecuellar@gmail.com |
| **TLP:** | **BLANCO** |
| **Registro grafico relacionado con el Phishing** | |



——— Forwarded message ———
De: **Jorge Enrique Cuellar Sanchez** <jorgeenriquecuellar@gmail.com>
Date: mar, 16 jul 2024 a las 10:47
Subject: VINCULACIÓN DEL POR ATRIBUCIÓN FISCAL,RADICADO: 20011-04562-59-2024-16072-00,
To:

16 Julio de 2024

E.S.D

Asunto: Apertura del Proceso 20011-02809-70-2024-16072-00
Debido a lo que establece la ley y con el fin de garantizar el debido proceso para todos los ciudadanos, nos permitimos notificarle de forma clara y concreta su vinculación al proceso de responsabilidad fiscal con radicado 20011-02809-70-2024-16072-00 por el cual usted figura como parte demanda como consecuencia del fraude realizado a los bienes pertenecientes al estado.

Adjunto acuerdo para que se presente al proceso de forma rápida y oportuna.

Adjunto protegido con contraseña: 0240716

VISUALIZAR ACUERDO DE PROCESO

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:** | REVISORDEDOCADJUNTODECITACDOCPDFRADIC20015-63289652-2024-79327492dpfpdf-gfs3658329652docadj346820001.pdf.exe |
| **Veredicto:** | **Actividad sospechosa** |
| **Fecha del análisis:** | Julio 16, 2024 at 12:05:11 |
| **MIME:** | application/x-dosexec |
| **Información del archivo:** | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| **MD5:** | 78896582E1E3B2E6C974FD0C651B37F0 |

| | |
|---|---|
| **SHA1:** | 29C4D32F4B990611B48E95DE294F64F43844FE6D |
| **SHA256:** | 879BBC7BF6A4C78BB4977CEE006D0796F8A39C69B6C7A3F8624F9D030EAAF437 |
| **SSDEEP:** | 98304:QKEzIqHAraFdWAkPvXvDXUloxB75tN1ukq6h9+RQG9Ey6PfkhXy+Rf4VfMcIgWS+:hQqrH |

Fuente. CSIRT Académico UNAD

**Información de proceso**

| CMD | Ruta Comprometida | Proceso Padre |
|---|---|---|
| "C:\Users\admin\AppData\Local\Temp\0200711c-0766-409c-8c2d-3f4e1c805693.exe" | "C:\Users\admin\AppData\Local\Temp\0200711c-0766-409c-8c2d-3f4e1c805693.exe" | explorer.exe |

Fuente. CSIRT Académico UNAD

Cordialmente

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