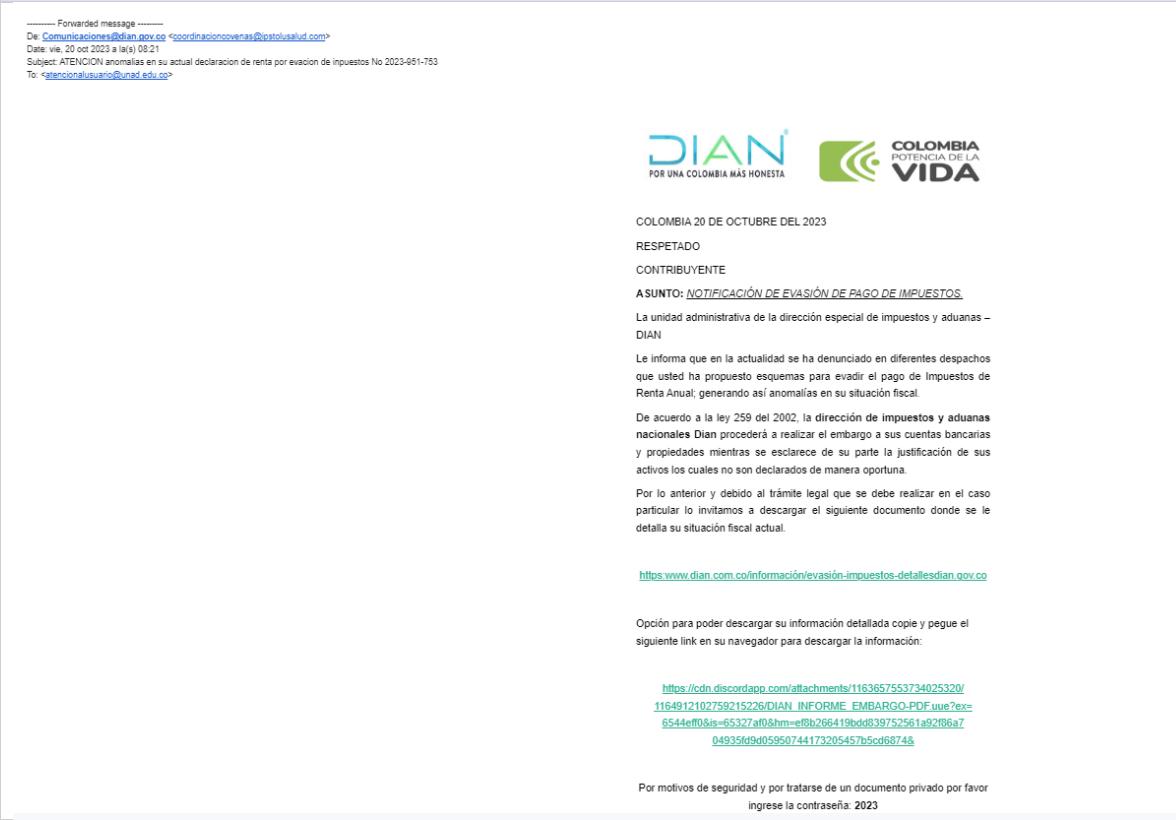
Boletín de Ciberseguridad

Octubre 20 de 2023

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	HEUR.Arch.Script.A
Cuenta de correo del remitente:	Comunicaciones@dian.gov.co <coordinacioncovenas@ipstolusalud.com>
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ---------
De: Comunicaciones@dian.gov.co <coordinacioncovenas@ipstolusalud.com>
Date: vie, 20 oct 2023 a la(s) 08:21
Subject: ATENCION anomalias en su actual declaracion de renta por evacion de inpuestos No 2023-951-753
To: <atencionalusuario@unad.edu.co>

DIAN
POR UNA COLOMBIA MÁS HONESTA

COLOMBIA POTENCIA DE LA VIDA

COLOMBIA 20 DE OCTUBRE DEL 2023

RESPETADO

CONTRIBUYENTE

ASUNTO: *NOTIFICACIÓN DE EVASIÓN DE PAGO DE IMPUESTOS.*

La unidad administrativa de la dirección especial de impuestos y aduanas – DIAN

Le informa que en la actualidad se ha denunciado en diferentes despachos que usted ha propuesto esquemas para evadir el pago de Impuestos de Renta Anual; generando así anomalías en su situación fiscal.

De acuerdo a la ley 259 del 2002, la **dirección de impuestos y aduanas nacionales Dian** procederá a realizar el embargo a sus cuentas bancarias y propiedades mientras se esclarece de su parte la justificación de sus activos los cuales no son declarados de manera oportuna.

Por lo anterior y debido al trámite legal que se debe realizar en el caso particular lo invitamos a descargar el siguiente documento donde se le detalla su situación fiscal actual.

https:www.dian.com.co/información/evasión-impuestos-detallesdian.gov.co

Opción para poder descargar su información detallada copie y pegue el siguiente link en su navegador para descargar la información:

https://cdn.discordapp.com/attachments/1163657553734025320/1164912102759215226/DIAN_INFORME_EMBARGO-PDF.uue?ex=6544eff0&is=65327af0&hm=ef8b266419bdd839752561a92f86a704935fd9d0595074417320545 7b5cd6874&

Por motivos de seguridad y por tratarse de un documento privado por favor ingrese la contraseña: **2023**

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:	DIAN_INFORME_EMBARGO-PDF.uue
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	October 20, 2023 at 16:53:25
MIME:	application/x-rar
Información del archivo:	RAR archive data, v5
MD5:	fe61d7fd96c0b248f5dc3c2e1df20141
SHA1:	6f51ab8128c2c8279798dfba875da0d945343b88
SHA256:	584c8cdfd5fb8a8534454ce24c6b794a577c45a7740b7da6bd20fc6a5de1e566
SSDEEP:	192:q2e+jnYl8HqBfYaEhqdeOzJlBFzQ8bscGUTIB6MWyIUIk+qhQe+CK2AQDKQxZN:qz+TUdYXhq8KTzQysvUAhWyIVkBWiYQb

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Program Files\WinRAR\WinRAR.exe" "C:\Users\admin\AppData\Local\Temp\DIAN_INFORME_EMBARGO-PDF.uue.rar"	C:\Program Files\WinRAR\WinRAR.exe	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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