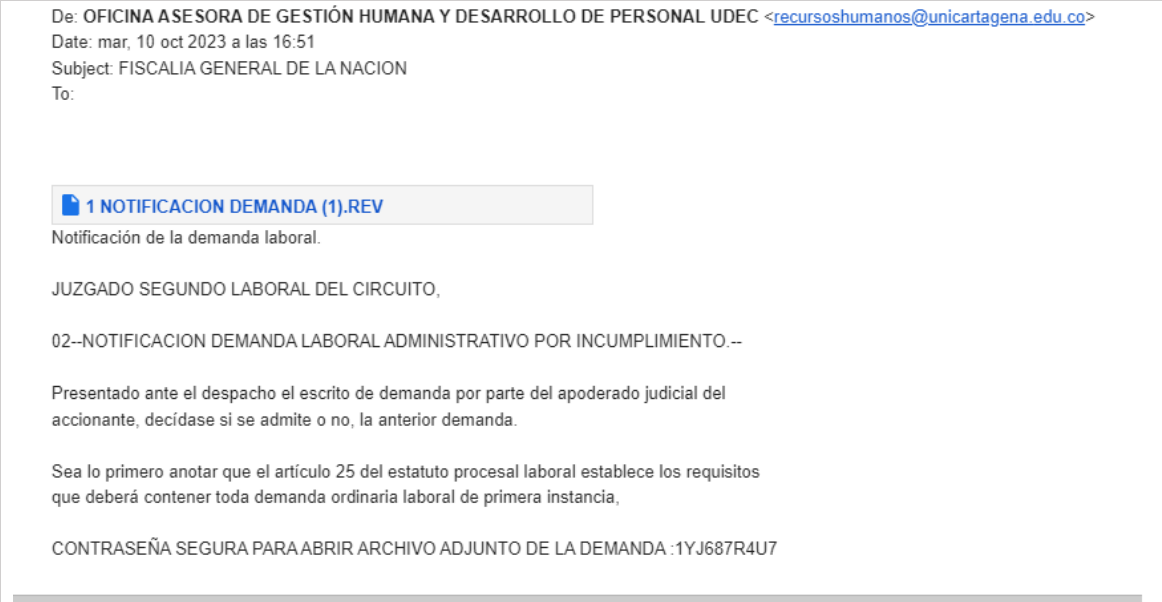
Octubre 11 de 2023

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	Trojan.U.AsyncRAT.bot
Cuenta de correo del remitente:	recursoshumanos@unicartagena.edu.co
TLP:	**BLANCO**

Registro grafico relacionado con el Phishing



De: **OFICINA ASESORA DE GESTIÓN HUMANA Y DESARROLLO DE PERSONAL UDEC** <recursoshumanos@unicartagena.edu.co>
Date: mar, 10 oct 2023 a las 16:51
Subject: FISCALIA GENERAL DE LA NACION
To:

1 NOTIFICACION DEMANDA (1).REV

Notificación de la demanda laboral.

JUZGADO SEGUNDO LABORAL DEL CIRCUITO,

02--NOTIFICACION DEMANDA LABORAL ADMINISTRATIVO POR INCUMPLIMIENTO.--

Presentado ante el despacho el escrito de demanda por parte del apoderado judicial del accionante, decídase si se admite o no, la anterior demanda.

Sea lo primero anotar que el artículo 25 del estatuto procesal laboral establece los requisitos que deberá contener toda demanda ordinaria laboral de primera instancia,

CONTRASEÑA SEGURA PARA ABRIR ARCHIVO ADJUNTO DE LA DEMANDA :1YJ687R4U7

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:	1 NOTIFICACION DEMANDA.EXE
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Octubre 11, 2023 at 22:28:15
MIME:	application/x-7z-compressed

Información del archivo:	7-zip archive data, version 0.4
MD5:	96aeb38d65c178166d089d70f189e5f7
SHA1:	3b5fd38214eae326030c52220e1b0d1d6d0c04d3
SHA256:	2c9e35a02103f6cd2a73b166ac0ec2bf7e1c39b9f7c046e3e6bb2e13be6bb981
SSDEEP:	49152:Z+PBKc4PZ60ydohpVaKANXRsE9dr/GQhjXcvncDyD4gs40:QPBKc4PZ6J7K0+E3DBXEncD8ns40

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Program Files\Windows Media Player\wmpnscfg.exe"	"C:\Program Files\Windows Media Player\wmpnscfg.exe"	wmpnscfg.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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