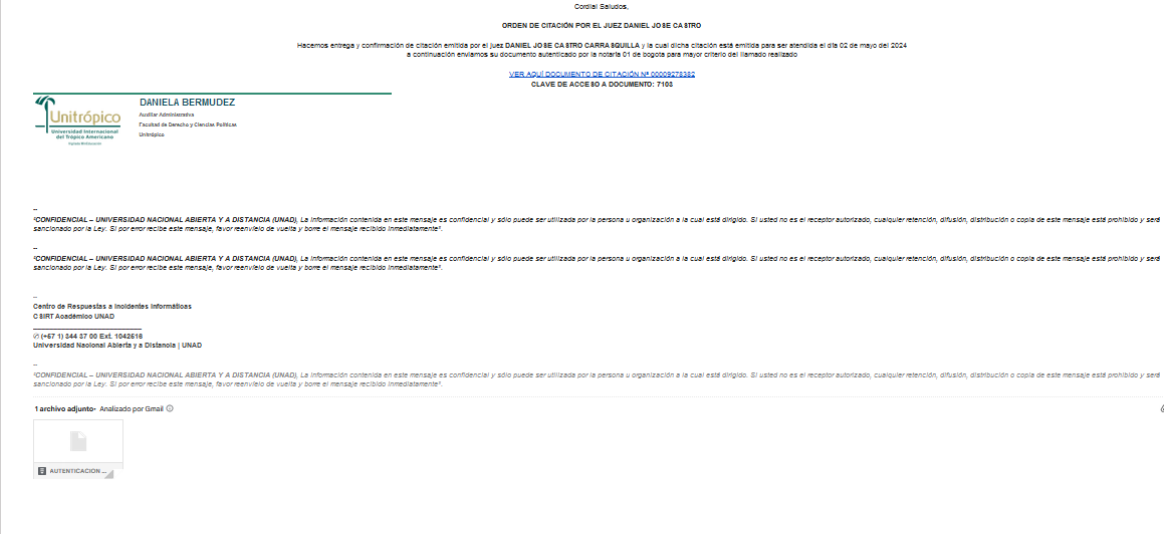
Mayo 02 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.remcos/zusy
Cuenta de correo del remitente:	**aux.derecho@unitropico.edu.co**
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	


Cordial Saludos,

ORDEN DE CITACIÓN POR EL JUEZ DANIEL JOSE CASTRO

Hacemos entrega y confirmación de citación emitida por el juez DANIEL JOSE CASTRO CARRASQUILLA y la cual dicha citación está emitida para ser atendida el día 02 de mayo del 2024
a continuación enviamos su documento autenticado por la notaría 01 de bogota para mayor criterio del llamado realizado

VER AQUÍ DOCUMENTO DE CITACIÓN Nº 00009278382
CLAVE DE ACCESO A DOCUMENTO: 7103

Unitrópico
DANIELA BERMUDEZ
Auxiliar Administrativo
Facultad de Derecho y Ciencias Políticas
Unitrópico

--
'CONFIDENCIAL – UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD). La información contenida en este mensaje es confidencial y sólo puede ser utilizada por la persona u organización a la cual está dirigido. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje está prohibido y será sancionado por la Ley. Si por error recibe este mensaje, favor reenviarlo de vuelta y borre el mensaje recibido inmediatamente'.

--
'CONFIDENCIAL – UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD). La información contenida en este mensaje es confidencial y sólo puede ser utilizada por la persona u organización a la cual está dirigido. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje está prohibido y será sancionado por la Ley. Si por error recibe este mensaje, favor reenviarlo de vuelta y borre el mensaje recibido inmediatamente'.

--
Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

(+57 1) 344 37 00 Ext. 1042616
Universidad Nacional Abierta y a Distancia | UNAD

--
'CONFIDENCIAL – UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD). La información contenida en este mensaje es confidencial y sólo puede ser utilizada por la persona u organización a la cual está dirigido. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje está prohibido y será sancionado por la Ley. Si por error recibe este mensaje, favor reenviarlo de vuelta y borre el mensaje recibido inmediatamente'.

1 archivo adjunto- Analizado por Gmail

AUTENTICACION ...

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:	AUTENTICACION DE PROCESO ANTES EL JUEZ DANIEL CASTRO.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Mayo 02, 2024 at 11:48:22
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	50119CF1DBE28B2F2441206269005DA1

SHA1:	73A228AB8EB8ADE45C194F2C8D4A9164C958758A
SHA256:	1DC3D117A22C53EE550654319AA82924EA0B134AA7C7BA3863F4940143008B19
SSDEEP:	98304:UutGyiq/DMQQh6otGIPnchkTM+qnKK+tPliFaJryo1:wOMyg

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\AUTENTICACION DE PROCESO ANTES EL JUEZ DANIEL CASTRO.exe"	"C:\Users\admin\AppData\Local\Temp\AUTENTICACION DE PROCESO ANTES EL JUEZ DANIEL CASTRO.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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