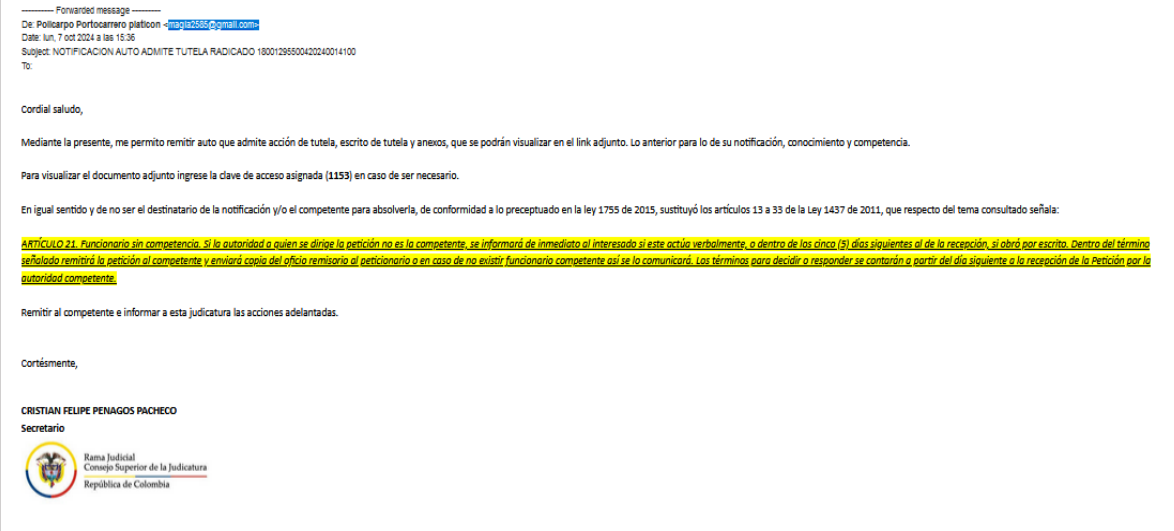
Octubre 08 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.ratx/remcos
Cuenta de correo del remitente:	magia2585@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ---------
De: Policarpo Portocarrero platicon <magia2585@gmail.com>
Date: lun, 7 oct 2024 a las 15:36
Subject: NOTIFICACION AUTO ADMITE TUTELA RADICADO 18001295500420240014100
To:

Cordial saludo,

Mediante la presente, me permito remitir auto que admite acción de tutela, escrito de tutela y anexos, que se podrán visualizar en el link adjunto. Lo anterior para lo de su notificación, conocimiento y competencia.

Para visualizar el documento adjunto ingrese la clave de acceso asignada (**1153**) en caso de ser necesario.

En igual sentido y de no ser el destinatario de la notificación y/o el competente para absolverla, de conformidad a lo preceptuado en la ley 1755 de 2015, sustituyó los artículos 13 a 33 de la Ley 1437 de 2011, que respecto del tema consultado señala:

ARTÍCULO 21. Funcionario sin competencia. Si la autoridad a quien se dirige la petición no es la competente, se informará de inmediato al interesado si este actúa verbalmente, o dentro de los cinco (5) días siguientes al de la recepción, si obró por escrito. Dentro del término señalado remitirá la petición al competente y enviará copia del oficio remisorio al peticionario o en caso de no existir funcionario competente así se lo comunicará. Los términos para decidir o responder se contarán a partir del día siguiente a la recepción de la Petición por la autoridad competente.

Remitir al competente e informar a esta judicatura las acciones adelantadas.

Cortésmente,

CRISTIAN FELIPE PENAGOS PACHECO
Secretario
Rama Judicial
Consejo Superior de la Judicatura
República de Colombia

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:	OfxTutelaRadicado18001295500420240014100.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	October 08, 2024 at 12:05:40
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	50E54F3131A1419A0FDAC1EC360F300D
SHA1:	26254B070E011DD49087D611184ED85AF9F1D740
SHA256:	7E5D3CA04246A2E61CCF5C307918079001015C5E6F5B1FEAA541423949EB444A

SSDEEP:	98304:9+MjIG3SfVSyyet+PCXXjMaeNuLGgookA1eiAvkRumXv:E

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\OfxTutelaRadicado18001295500420240014100.exe"	"C:\Users\admin\AppData\Local\Temp\OfxTutelaRadicado18001295500420240014100.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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