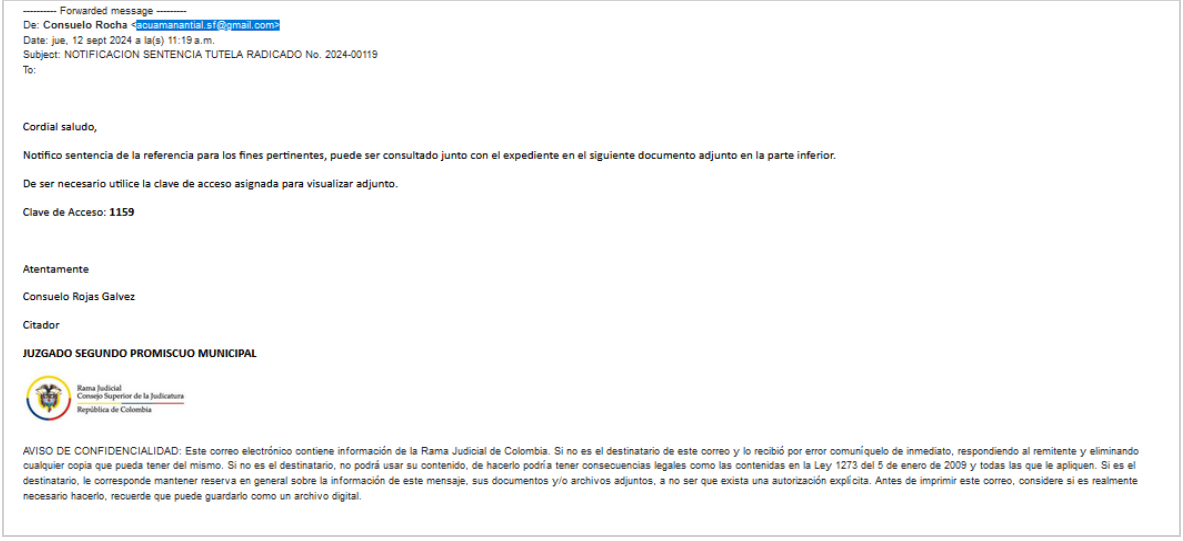
Septiembre 13 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.remcos
Cuenta de correo del remitente:	acuamanantial.sf@gmail.com
TLP:	**BLANCO**

Registro grafico relacionado con el Phishing



---------- Forwarded message ---------
De: **Consuelo Rocha** <acuamanantial.sf@gmail.com>
Date: jue, 12 sept 2024 a la(s) 11:19 a.m.
Subject: NOTIFICACION SENTENCIA TUTELA RADICADO No. 2024-00119
To:

Cordial saludo,

Notifico sentencia de la referencia para los fines pertinentes, puede ser consultado junto con el expediente en el siguiente documento adjunto en la parte inferior.

De ser necesario utilice la clave de acceso asignada para visualizar adjunto.

Clave de Acceso: **1159**

Atentamente

Consuelo Rojas Galvez

Citador

JUZGADO SEGUNDO PROMISCUO MUNICIPAL

Rama Judicial
Consejo Superior de la Judicatura
República de Colombia

AVISO DE CONFIDENCIALIDAD: Este correo electrónico contiene información de la Rama Judicial de Colombia. Si no es el destinatario de este correo y lo recibió por error comuníquelo de inmediato, respondiendo al remitente y eliminando cualquier copia que pueda tener del mismo. Si no es el destinatario, no podrá usar su contenido, de hacerlo podría tener consecuencias legales como las contenidas en la Ley 1273 del 5 de enero de 2009 y todas las que le apliquen. Si es el destinatario, le corresponde mantener reserva en general sobre la información de este mensaje, sus documentos y/o archivos adjuntos, a no ser que exista una autorización explícita. Antes de imprimir este correo, considere si es realmente necesario hacerlo, recuerde que puede guardarlo como un archivo digital.

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:	Ofx053Sentenc1aTutelaRad20240011900170424089002.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Septiembre 13, 2024 at 11:55:07
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	065866D9688C615F08F59398A005D109

SHA1:	8600BF76B41CA18883FECB0142D5EE5A8E8C1EA7
SHA256:	058EE523D41E2D442F72E975C9E400733296A6DDF46DCCAB4813177766BDCF43
SSDEEP:	49152:bw4sOCfwD94aWUG2T/ZJsbKBPBAH7GJL7G2bRMbg0quAwaWAx8KJT/er2xMVS2Jl:brsFbKBPBA+mGKhLcT/epVTzbT

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\Ofx053Sentenc1aTutelaRad20240011900170424089002.exe"	"C:\Users\admin\AppData\Local\Temp\Ofx053Sentenc1aTutelaRad20240011900170424089002.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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