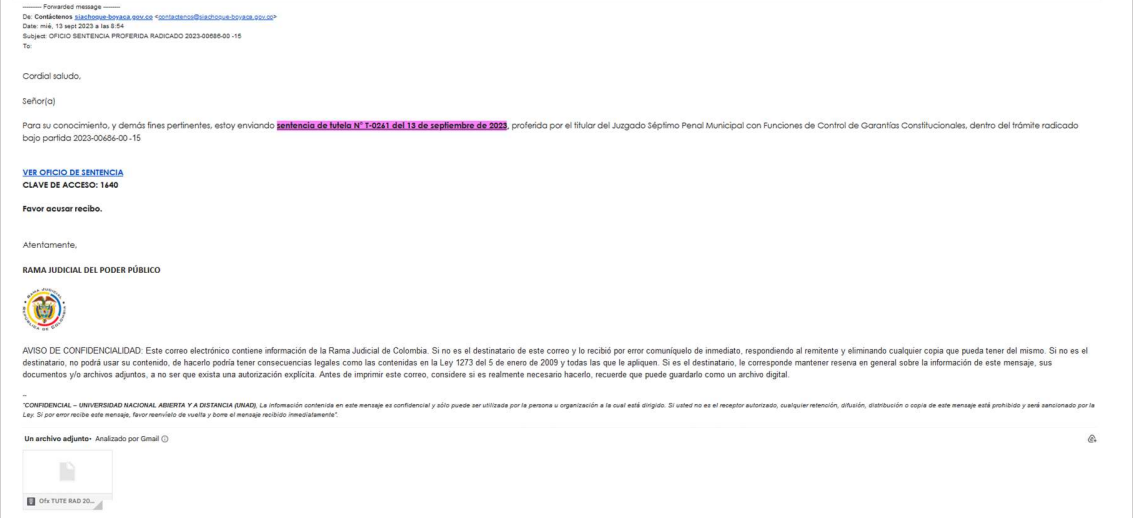
Septiembre 14 de 2023

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.msil/blocker
Cuenta de correo del remitente:	siachoque-boyaca.gov.co contactenos@siachoque-boyaca.gov.co
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ---------
De: **Contáctenos** siachoque-boyaca.gov.co <contactenos@siachoque-boyaca.gov.co>
Date: mié, 13 sept 2023 a las 8:54
Subject: OFICIO SENTENCIA PROFERIDA RADICADO 2023-00686-00 -15
To:

Cordial saludo,

Señor(a)

Para su conocimiento, y demás fines pertinentes, estoy enviando **sentencia de tutela N° T-0241 del 13 de septiembre de 2023**, proferida por el titular del Juzgado Séptimo Penal Municipal con Funciones de Control de Garantías Constitucionales, dentro del trámite radicado bajo partida 2023-00686-00 -15

VER OFICIO DE SENTENCIA
CLAVE DE ACCESO: 1640

Favor acusar recibo.

Atentamente,

RAMA JUDICIAL DEL PODER PÚBLICO

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.

--
"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".

Un archivo adjunto- Analizado por Gmail

Ofx TUTE RAD 20...

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:	Ofx TUTE RAD 2023-00686-00 -15.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	September 14, 2023 at 11:28:15
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5:	2405D5DCCAA91C9A38B45978C45A2839

SHA1:	52684755E142E4DB03DB3EBE5936BB146FA50741
SHA256:	C25CCCB64D855D1DD3AF6ECFF3FB8CD34637F05E2E75D37FCDFFDC739A8788E6
SSDEEP:	98304:0e6rzjm1HYh4tffpqfR+EZUbxmhUs5/z9BCs6L3ganlakkZuWDE:0xXjm14h4tfBURUbMCK/xBCs6L3gvkvl

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\Ofx TUTE RAD 2023-00686-00 -15.exe"	C:\Users\admin\AppData\Local\Temp\Ofx TUTE RAD 2023-00686-00 -15.exe	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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