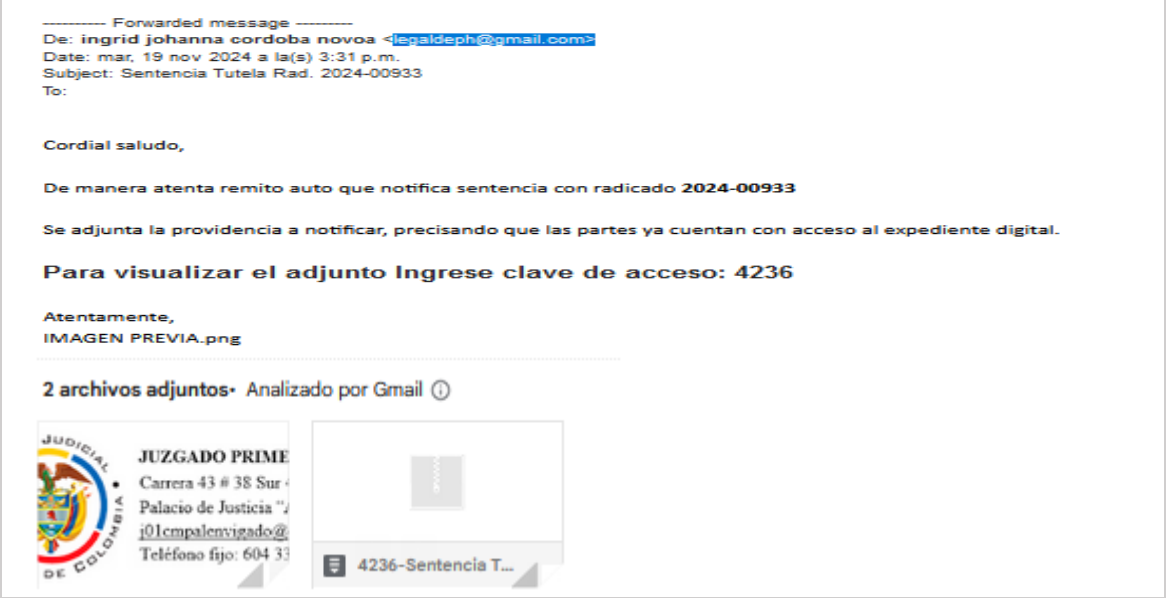
Noviembre 22 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

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



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:	4236-Sentencia Tutela Rad. 2024-00933.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	November 22, 2024 at 09:38:55
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections
MD5:	C8ACE54E5428AD4788B79882E4AAFBFC

SHA1:	E54CE6772B4972B1757158AEB0D31BEF8440CE43
SHA256:	7FA10347D61C120F616D7947F94F74F5E9DA2A9F056D6B2E9BFFA28484F7659C
SSDEEP:	24576:ZaRyTFTjEPx2xLzITVWG0oQq9hIExyZAQAqxm5233:ZaU5TjEPx2xLzITVWG0oQq9hIExyZxNt

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\4236-Sentencia Tutela Rad. 2024-00933.exe"	"C:\Users\admin\AppData\Local\Temp\4236-Sentencia Tutela Rad. 2024-00933.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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