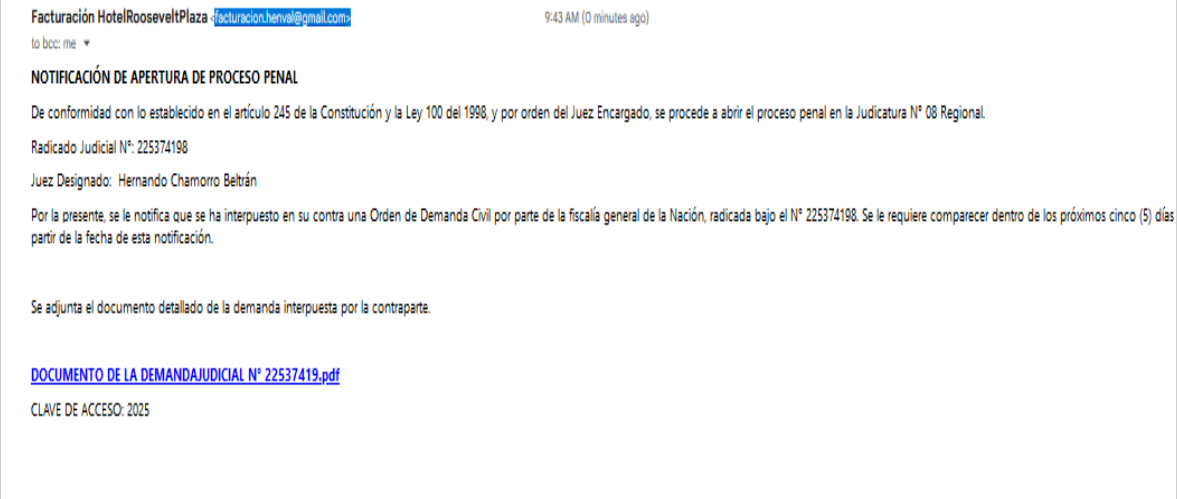
Octubre 31 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

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



Facturación HotelRooseveltPlaza <facturacion.henval@gmail.com> 9:43 AM (0 minutes ago)

to bcc: me

NOTIFICACIÓN DE APERTURA DE PROCESO PENAL

De conformidad con lo establecido en el artículo 245 de la Constitución y la Ley 100 del 1998, y por orden del Juez Encargado, se procede a abrir el proceso penal en la Judicatura N° 08 Regional.

Radicado Judicial N°: 225374198

Juez Designado: Hernando Chamorro Beltrán

Por la presente, se le notifica que se ha interpuesto en su contra una Orden de Demanda Civil por parte de la fiscalía general de la Nación, radicada bajo el N° 225374198. Se le requiere comparecer dentro de los próximos cinco (5) días partir de la fecha de esta notificación.

Se adjunta el documento detallado de la demanda interpuesta por la contraparte.

DOCUMENTO DE LA DEMANDAJUDICIAL N° 22537419.pdf

CLAVE DE ACCESO: 2025

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:	Acuerdo_Legal.N°93782672..exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	October 31, 2024 at 15:36:33
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows, 8 sections
MD5:	F7ACD12CD25F70495880816C42BB320B
SHA1:	D1978987D2E7FF7FF364774E273BFC318EB00C76
SHA256:	8DC7FBDFAC755D60CE05B1C223C174BA13ABD78EB01AA538B37C0B812ECE3AA5

SSDEEP:	49152:lilP/Ti7paMepaRsH6XjaIxmeqxOYnYAotG24DB84k9kGOddRsZVLq7S6uyzc2y8:Qisysuoh9hdy+1

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\Acuerdo_Legal.N°93782672..exe"	"C:\Users\admin\AppData\Local\Temp\Acuerdo_Legal.N°93782672..exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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