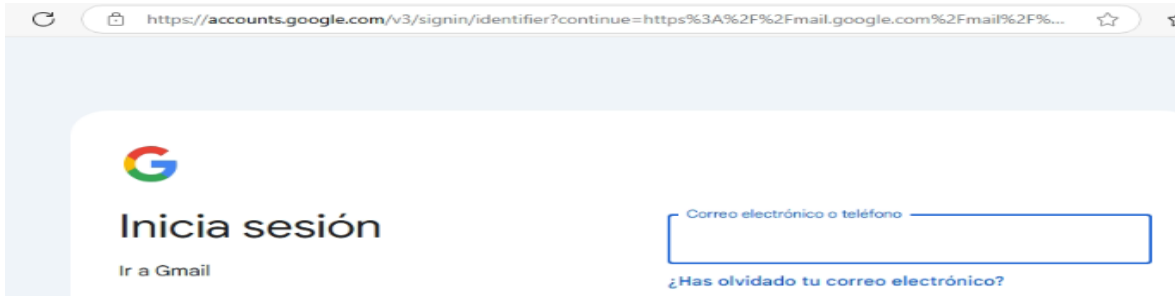


Boletín de Ciberseguridad

Noviembre 13 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	no se evidencia
Cuenta de correo del remitente:	jairotoro65@gmail.com
TLP:	BLANCO
Registro grafico relacionado con el Phishing	
----- Forwarded message ----- De: EMAIL CERTIFICADO DE LA RAMA JUDICIAL DEL PODER PÚBLICO DE LA REPÚBLICA DE COLOMBIA CENDO NOTIF3 <jairotoro65@gmail.com> Date: mié, 6 nov 2024 a la(s) 1:04 p.m. Subject: J8924 /// NOTIFIQUESE Y CÚMPLASE /// CENDO RAMA JUDICIAL /// AUTO ADMISORIO DEMANDA LABORAL /// J8924 To: J8924 /// NOTIFIQUESE Y CÚMPLASE /// CENDO RAMA JUDICIAL /// AUTO ADMISORIO DEMANDA LABORAL /// J8924 RAMA JUDICIAL DEL PODER PÚBLICO REPÚBLICA DE COLOMBIA CLAVE DE ARCHIVO: 06NOV2024ESM 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, bajo la modalidad de Smishing, donde se recibe un correo, para que el receptor tome contacto con una supuesta entidad con el fin de obtener 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.

Boletín de Ciberseguridad

Por lo cual se recomienda no ingresar sus Credenciales, cuando lleguen mensajes de una supuestamente **J8924 /// NOTIFÍQUESE Y CÚMPLASE /// CENDO RAMA JUDICIAL /// AUTO ADMISORIO DEMANDA LABORAL /// J8924**. donde adjuntan un documento.

Pero esta te redirecciona a esta página

https://accounts.google.com/v3/signin/identifier?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F%3Fui%3D2%26ik%3D4a5f54ecae%26attid%3D0.1%26permmsgid%3Dmsg-f%3A1815472704242967373%26th%3D1931dace43d1e34d%26view%3Datt%26disp%3Dsafe%26realattid%3Df_m366rb8j0%26zw&emr=1&ifkv=AcMMx-dMAT1s-3ogCKVmy2FNkmBzrNJcvQBo6C3HKpanVePMID8kyuplCFqchl_Zh0mwbZ_YFoc0Ag<mpl=default<mplcache=2&osid=1&passive=true&rm=false&scc=1&service=mail&flowName=GlifWebSignIn&flowEntry=ServiceLogin&dsh=S-905567522%3A1731505211571723&ddm=1

como se ve en la imagen la cual es completamente diferente. La cual pide credenciales de GMAIL con el fin de acceder o robar su información.

Fuente. CSIRT Académico UNAD

Cordialmente

CSIRT Académico UNAD

Correo electrónico: csirt@unad.edu.co

(+57 1) 344 37 00 Ext. 1042516