Octubre 24 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:	j03mpmixartado@cendoj.ramajudicial.gov.co
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, 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.

Por lo cual se recomienda no ingresar sus Credenciales, cuando lleguen mensajes de una supuestamente **0354005-NOTIFICACION DEMANDA LABORAL JUZGADO 03 PENAL DEL CIRCUITO DE RAMA JUDICIAL -0654700** 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%3A1813806681970996098%26th%3D192bef913a1c7382%26view%3Datt%26disp%3Dsafe%26realattid%3D192b4de1cfd9caf3ce21&emr=1&ifkv=AcMMx-fCyLa6dW4fniH9KHu4rlwvbke1dktj9Q5eInxCk7giAsEa0EKqVMXrLeSt4xCTe8rTl8vbCg&ltmpl=default&ltmplcache=2&osid=1&passive=true&rm=false&scc=1&service=mail&flowName=GlifWebSignIn&flowEntry=ServiceLogin&dsh=S774737217%3A1729787721579042&ddm=0

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

Fuente. CSIRT Académico UNAD

Cordialmente

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