



Boletín de Ciberseguridad

Octubre 03 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:	competitividad@lavirginia-risaralda.gov.co
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 SENDO RAMAJ2 <competitividad@lavirginia-risaralda.gov.co>
 Date: mié, 2 oct 2024 a las 7:17 p.m.
 Subject: 789194813 NOTIFICACIÓN DE EJECUCIÓN COACTIVA - ORDEN DE EMBARGO - SENDO RAMA JUDICIAL 789194813
 To:


789194813 NOTIFICACIÓN DE EJECUCIÓN COACTIVA - ORDEN DE EMBARGO - SENDO RAMA JUDICIAL 789194813
 MEDIANTE ARCHIVO ADJUNTO NOS PERMITIMOS REMITIR SENTENCIA.
 CLAVE DE ARCHIVO: 02OCT2024ESM

 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 reenvíelo de vuelta y borrar el mensaje recibido inmediatamente.

 Centro de Respuestas a Incidentes Informáticas
 CSIRT Académico UNAD
 ☎ (+57 1) 344 37 00 Ext. 1042516
 Universidad Nacional Abierta y a Distancia | UNAD

 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 reenvíelo de vuelta y borrar el mensaje recibido inmediatamente.

1 archivo adjunto - Analizado por Gmail



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.



Boletín de Ciberseguridad

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 **789194813** ::::::::::: **NOTIFICACIÓN DE EJECUCIÓN COACTIVA - ORDEN DE EMBARGO - SENDO RAMA JUDICIAL** ::::::::::: **789194813**, 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%3A1811927621606958534%26th%3D192542926499e5c6%26view%3Datt%26disp%3Dsafe%26realattid%3Df_m1sjq4u60&emr=1&ifkv=ARpgrqeDnunclRz-4bH620m5QiyLBK9RCV9LE7AGINKjggjrWawWxqSQCK8cFACrXa1uinA4UnA<mpl=default<mplcache=2&osid=1&passive=true&rm=false&sc=1&service=mail&flowName=GlifWebSignIn&flowEntry=ServiceLogin&dsh=S1361861039%3A1727991840163671&ddm=1

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