

Boletín de Ciberseguridad

Octubre 08 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:	magianet1713@gmail.com
TLP:	BLANCO

Registro grafico relacionado con el Phishing

----- Forwarded message -----
 De: MARIANY GIANIY <magianet1713@gmail.com>
 Date: lun, 7 oct 2024 a las 15:49
 Subject: NOTIFICACIÓN FALLO TUTELA RADICADO 04740 89001 2024 00203
 To:

Cordial saludo;

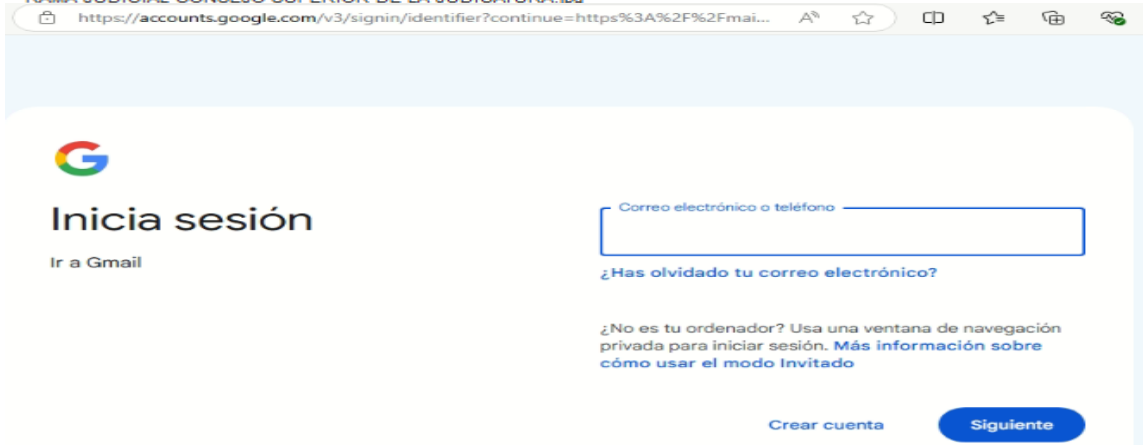
Atentamente, me permito notificar el fallo de la acción de tutela del radicado de referencia.

En la parte inferior encontrara documento adjunto, con folios y escrito de tutela.

El documento a visualizar cuenta con clave de acceso: **1153**

FAVOR ACUSAR RECIBO.

Atte.
 MARIA JENNY HERNANDEZ SUAREZ
 Escribiente
 Juzgado Promiscuo Municipal
 RAMA JUDICIAL CONSEJO SUPERIOR DE LA JUDICATURA, los



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 **NOTIFICACIÓN FALLO TUTELA RADICADO 04740 89001 2024 00203**, 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%3A1812364634349266098%26th%3D1926d00859de64b2%26view%3Datt%26disp%3Dsafe%26realattid%3Dii_m1zhaj590&emr=1&ifkv=ARpgrqdh8e-EBCeW-0-rl3JcL0X1e7cZDZHWr5iiFbgF3eGxMMht4QJpWKcMJd16Ap6YPHTkLUBpjA<mpl=default<mplcache=2&osid=1&passive=true&rm=false&scc=1&service=mail&flowName=GlifWebSignIn&flowEntry=ServiceLogin&dsh=S-1507453595%3A1728406058500033&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