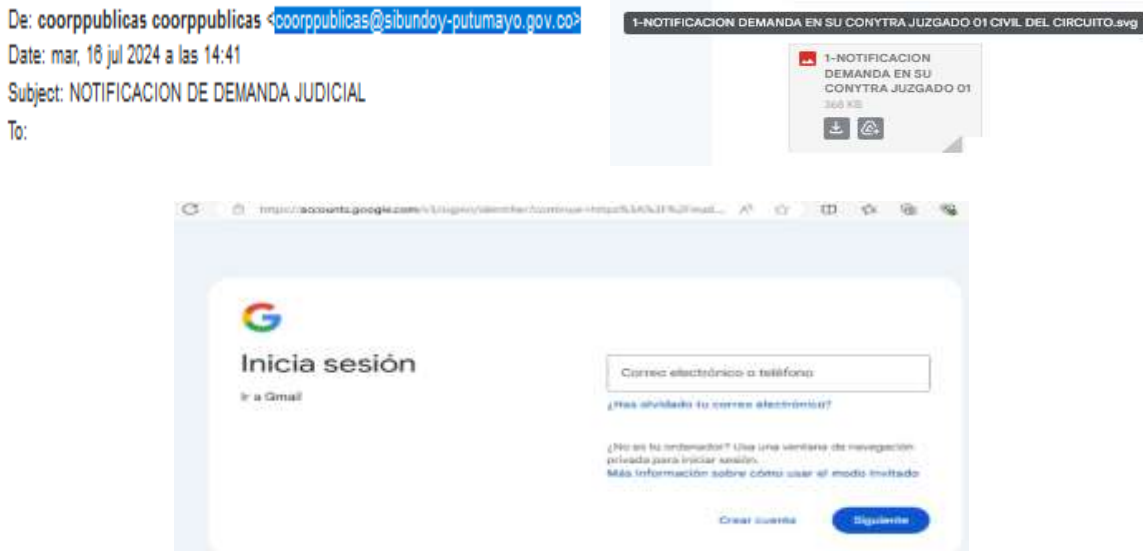


Boletín de Ciberseguridad

Julio 16 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:	coorppublicas@sibundoy-putumayo.gov.co
TLP:	BLANCO
Registro grafico relacionado con el Phishing	
 The image shows a screenshot of a phishing email and a corresponding fake login page. The email header indicates it is from 'coorppublicas@sibundoy-putumayo.gov.co' with the subject 'NOTIFICACION DE DEMANDA JUDICIAL'. The email body contains a link to a fake Google login page. The login page mimics the Google interface, asking for an email address or phone number to log in. A download icon for a file named '1-NOTIFICACION DEMANDA EN SU CONYTRA JUZGADO 01 CIVIL DEL CIRCUITO.svg' is also visible.	

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 NOTIFICACION DE DEMANDA JUDICIAL, donde adjuntan un PDF. y 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%3A1804768860679358560%26th%3D190bd3b77a7ac860%26view%3Datt%26disp%3Dsafe%26realattid%3Df_lyotk61s0&emr=1&ifkv=AdF4I7727VZUGPDB_JOz9o6qJdShSrlhqsorsiwVpSIWIoTOEjO6XPQhuy4ZiOUqrF93SuZCtpbWg<mpl=default<mplcache=2&osid=1&passive=true&rm=false&sc=1&service=mail&flowName=GlifWebSignIn&flowEntry=ServiceLogin&dsh=S-1357915344%3A1721165625770083&ddm=0, como se ve en la imagen completamente diferente. Y es algo totalmente diferente donde te piden ingresar tus datos de correo electrónico.

Con el fin de que su información no sea robada. Por esta razón lo deben de realizar directamente en las páginas principales

Fuente. CSIRT Académico UNAD

Cordialmente

CSIRT Académico UNAD

Correo electrónico: csirt@unad.edu.co

(+57 1) 344 37 00 Ext. 1042516