

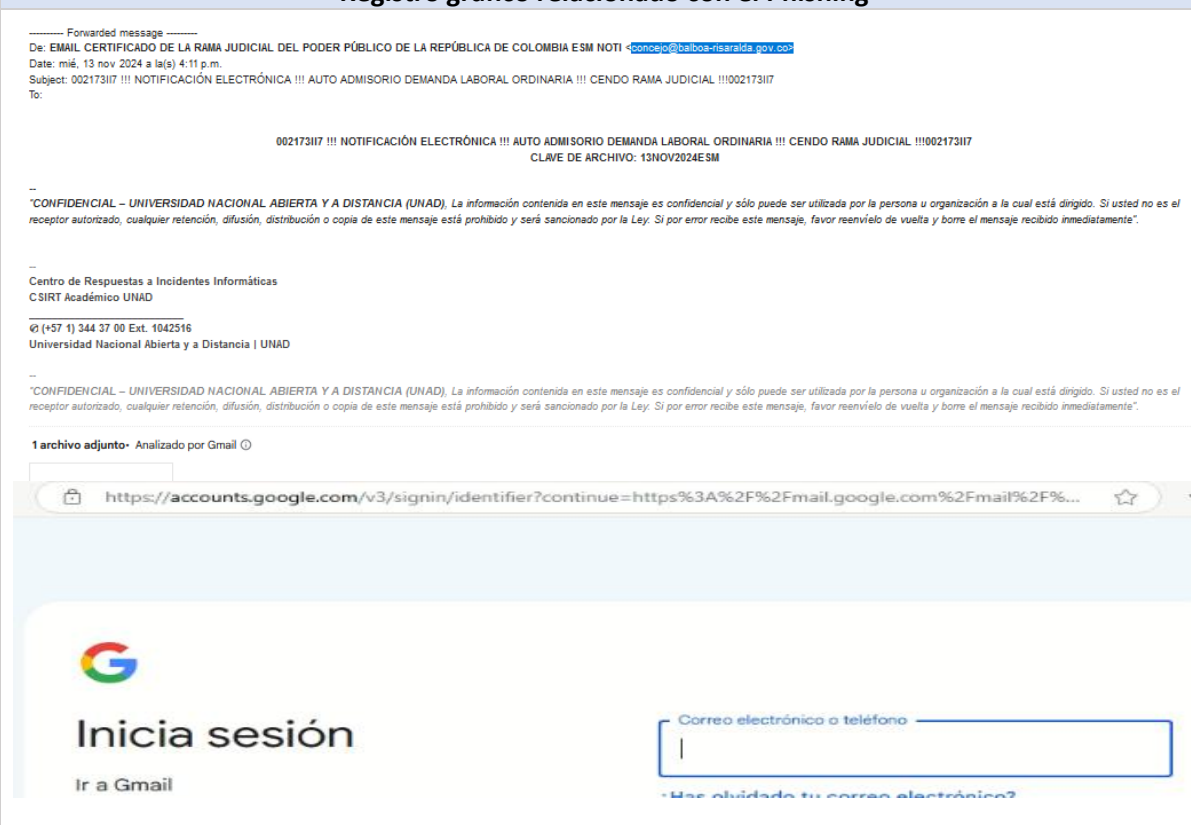
Boletín de Ciberseguridad

Noviembre 15 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:	concejo@balboa-risaralda.gov.co
TLP:	BLANCO

Registro grafico relacionado con el Phishing



The image shows a screenshot of a phishing email and the Google login page. The email header indicates it is a forwarded message from 'concejo@balboa-risaralda.gov.co' dated 13 nov 2024 at 4:11 p.m. The subject is '002173117 !!! NOTIFICACIÓN ELECTRÓNICA !!! AUTO ADMISORIO DEMANDA LABORAL ORDINARIA !!! CENDO RAMA JUDICIAL !!!002173117'. The body of the email contains a 'CONFIDENCIAL' notice from UNAD, a contact for the CSIRT Académico UNAD, and another 'CONFIDENCIAL' notice. Below the email, there is a screenshot of the Google login page with the URL 'https://accounts.google.com/v3/signin/identifier?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F%...' and the text 'Inicia sesión' and 'Ir a 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.

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 **002173II7 !!! NOTIFICACIÓN ELECTRÓNICA !!! AUTO ADMISORIO DEMANDA LABORAL ORDINARIA !!! CENDO RAMA JUDICIAL !!!002173II7**. 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%3A1815799073717031043%26th%3D193303a314631083%26view%3Datt%26disp%3Dsafe%26realattid%3Df_m3gdkq6o0%26zw&emr=1&ifkv=AcMMx-daQfa-8VocSEGr4im4rRes9Puyabydph5smvBpLBWHICZ9ka-Y2Z2oMxRSu9eguqp235Jt-A<mpl=default<mplcache=2&osid=1&passive=true&rm=false&scc=1&service=mail&flowName=GlifWebSignIn&flowEntry=ServiceLogin&dsh=S-938744529%3A1731688851492158&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