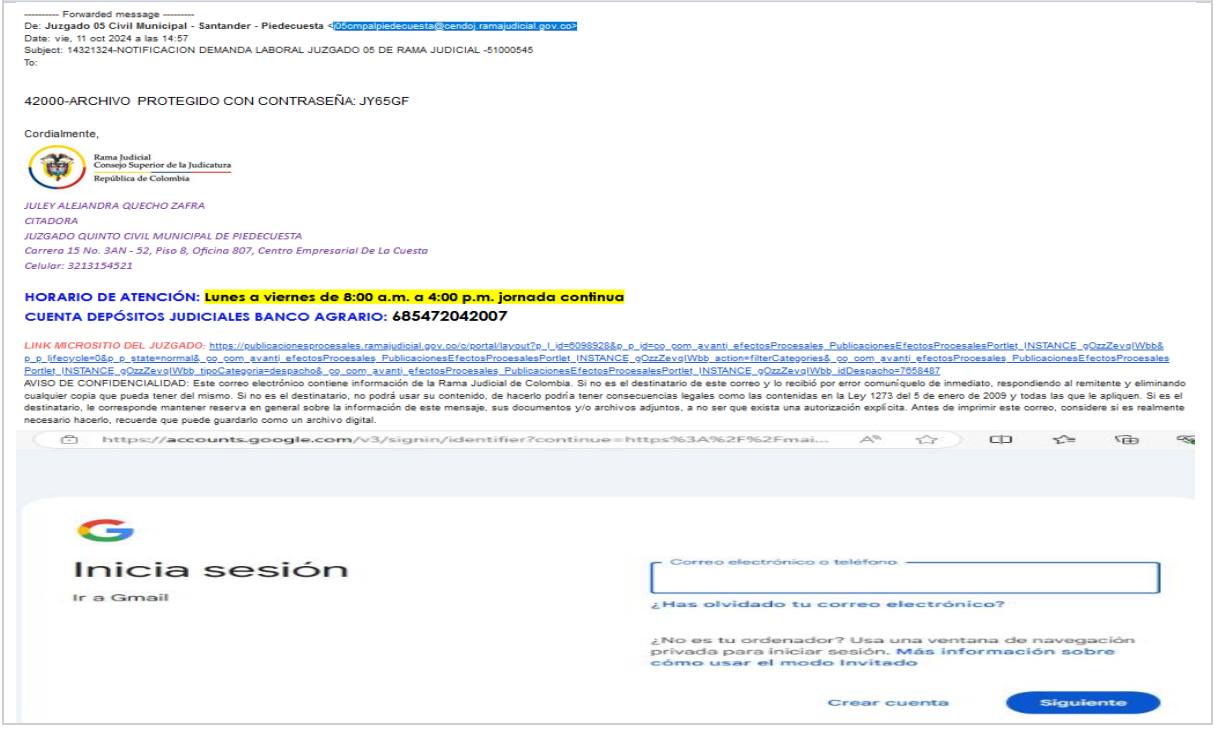
Octubre 15 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	no se evidencia
Cuenta de correo del remitente:	j05cmpalpiedecuesta@cendoj.ramajudicial.gov.co
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ---------
De: **Juzgado 05 Civil Municipal - Santander - Piedecuesta** <j05cmpalpiedecuesta@cendoj.ramajudicial.gov.co>
Date: vie, 11 oct 2024 a las 14:57
Subject: 14321324-NOTIFICACION DEMANDA LABORAL JUZGADO 05 DE RAMA JUDICIAL -51000545
To:

42000-ARCHIVO PROTEGIDO CON CONTRASEÑA: JY65GF

Cordialmente,

Rama Judicial
Consejo Superior de la Judicatura
República de Colombia

JULEY ALEJANDRA QUECHO ZAFRA
CITADORA
JUZGADO QUINTO CIVIL MUNICIPAL DE PIEDECUESTA
Carrera 15 No. 3AN - 52, Piso 8, Oficina 807, Centro Empresarial De La Cuesta
Celular: 3213154521

HORARIO DE ATENCIÓN: Lunes a viernes de 8:00 a.m. a 4:00 p.m. jornada continua
CUENTA DEPÓSITOS JUDICIALES BANCO AGRARIO: 685472042007

LINK MICROSITIO DEL JUZGADO: https://publicacionesprocesales.ramajudicial.gov.co/p/portal/layout?p_l_id=60988288&p_p_id=co_com_avanti_efectosProcesales_PublicacionesEfectosProcesalesPortlet_INSTANCE_qOzzZevqIWbb&p_p_lifecycle=0&p_p_state=normal&_co_com_avanti_efectosProcesales_PublicacionesEfectosProcesalesPortlet_INSTANCE_qOzzZevqIWbb_action=filterCategories&_co_com_avanti_efectosProcesales_PublicacionesEfectosProcesalesPortlet_INSTANCE_qOzzZevqIWbb_tipoCategoria=despacho&_co_com_avanti_efectosProcesales_PublicacionesEfectosProcesalesPortlet_INSTANCE_qOzzZevqIWbb_idDespacho=7658487

AVISO DE CONFIDENCIALIDAD: Este correo electrónico contiene información de la Rama Judicial de Colombia. Si no es el destinatario de este correo y lo recibió por error comuníquelo de inmediato, respondiendo al remitente y eliminando cualquier copia que pueda tener del mismo. Si no es el destinatario, no podrá usar su contenido, de hacerlo podría tener consecuencias legales como las contenidas en la Ley 1273 del 5 de enero de 2009 y todas las que le apliquen. Si es el destinatario, le corresponde mantener reserva en general sobre la información de este mensaje, sus documentos y/o archivos adjuntos, a no ser que exista una autorización explícita. Antes de imprimir este correo, considere si es realmente necesario hacerlo, recuerde que puede guardarlo como un archivo digital.

https://accounts.google.com/v3/signin/identifier?continue=https%3A%2F%2Fmai...

Inicia sesión
Ir a Gmail

Correo electrónico o teléfono
¿Has olvidado tu correo electrónico?
¿No es tu ordenador? Usa una ventana de navegación privada para iniciar sesión. Más información sobre cómo usar el modo Invitado
Crear cuenta
Siguiente

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 **14321324-NOTIFICACION DEMANDA LABORAL JUZGADO 05 DE RAMA JUDICIAL - 51000545,** 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%3A1812940409426492016%26th%3D1928dbb26ed13a70%26view%3Datt%26disp%3Dsafe%26realattid%3D1927d781ab29f1281842&emr=1&ifkv=ARpgrqf9tG9_p9MbXm8xL6cAzoy_SbWZ9JbWLy5NeBcPP9Hyjs0V2DqB4qa3zPBmfHcsSOMlS9RK2g&ltmpl=default&ltmplcache=2&osid=1&passive=true&rm=false&scc=1&service=mail&flowName=GlifWebSignIn&flowEntry=ServiceLogin&dsh=S-618022986%3A1729001272607014&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