

Boletín de Ciberseguridad

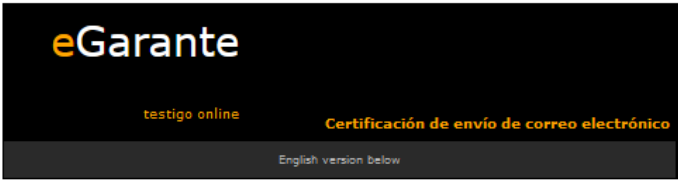
Diciembre 17 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	no se evidencia
Cuenta de correo del remitente:	mailsigned@egarante.com
TLP:	BLANCO

Registro grafico relacionado con el Phishing

----- Forwarded message -----
 De: MailSigned <mailsigned@egarante.com>
 Date: lun, 16 de dic de 2024, 10:20 a. m.
 Subject: [eGarante] Certificación de envío de correo electrónico (Certified email) asunto: Reporte de Incidente Tecnológico y Error con Notas en Plataforma AUREA
 To: Carlos Eduardo Ricaurte Gallo <ceduardo958@soy.sena.edu.co>
 Cc: Coordinación Académica JAG <academica.zcbc@unad.edu.co>



Estimado Sr./Sra.:

ceduardo958@soy.sena.edu.co ha solicitado a eGarante actuar como testigo del envío del correo electrónico con el asunto: Reporte de Incidente Tecnológico y Error con Notas en Plataforma AUREA.

Adjuntamos en este correo un documento en pdf firmado electrónicamente con la certificación de dicho envío. Esta certificación es entregada tanto al emisor como a todos los destinatarios del correo: Coordinación Académica JAG <academica.zcbc@unad.edu.co>.

La primera página de la certificación contiene las características esenciales del envío y a partir de la página 2 encontrará la transcripción exacta y fiel de la información intercambiada por los servidores de correo electrónico con la que se puede reconstruir el mensaje original.

Para facilitar la correspondencia de la certificación con el correo que la ha originado hemos adjuntado una copia del mensaje original a este correo en formato .eml que puede ser leído con el programa de correo electrónico gratuito Mozilla Thunderbird



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

Boletín de Ciberseguridad

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 **[eGarante] Certificación de envío de correo electrónico (Certified email) asunto: Reporte de Incidente Tecnológico y Error con Notas en Plataforma AUREA.** 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%3D0.2%26permmsgid%3Dmsg-f%3A1818716098618090842%26th%3D193d60a7dd6a655a%26view%3Datt%26disp%3Dsafe%26realattid%3D193d57c39c78928ff472%26zw&emr=1&ifkv=AeZLP9_2q_8rZv0wyQStSiZEehC3HWX4vAUSMeZygQ3-JvN2wQQIgnBFa1Uq-LxtA31Ht2lo-FBI0Q<mpl=default<mplcache=2&osid=1&passive=true&rm=false&scc=1&service=mail&flowName=GlifWebSignIn&flowEntry=ServiceLogin&dsh=S892631841%3A1734470538277953&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