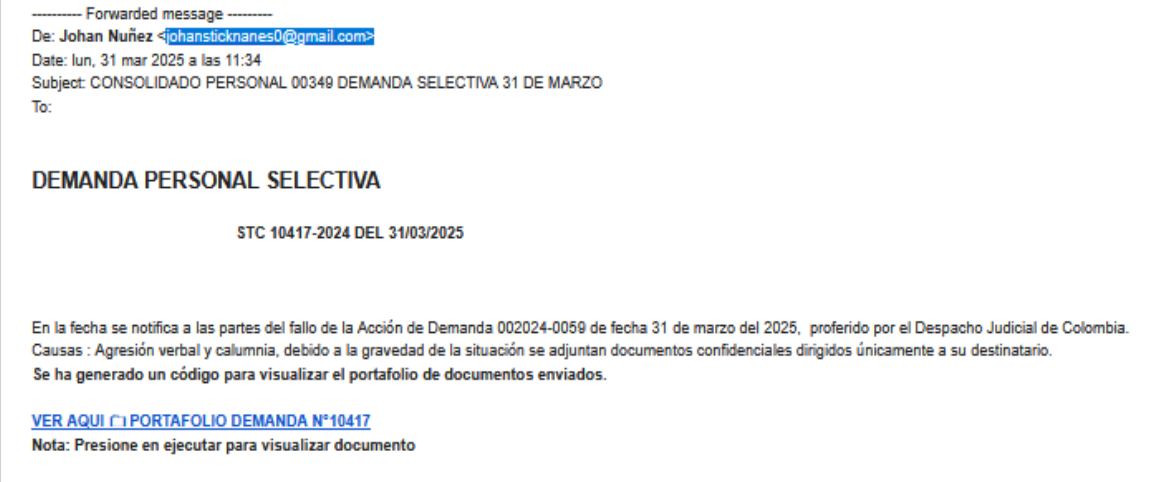
Marzo 31 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.brresmon
Cuenta de correo del remitente:	johansticknanes0@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ---------
De: **Johan Nuñez** <johansticknanes0@gmail.com>
Date: lun, 31 mar 2025 a las 11:34
Subject: CONSOLIDADO PERSONAL 00349 DEMANDA SELECTIVA 31 DE MARZO
To:

DEMANDA PERSONAL SELECTIVA

STC 10417-2024 DEL 31/03/2025

En la fecha se notifica a las partes del fallo de la Acción de Demanda 002024-0059 de fecha 31 de marzo del 2025, proferido por el Despacho Judicial de Colombia.
Causas : Agresión verbal y calumnia, debido a la gravedad de la situación se adjuntan documentos confidenciales dirigidos únicamente a su destinatario.
Se ha generado un código para visualizar el portafolio de documentos enviados.

VER AQUI PORTAFOLIO DEMANDA N°10417
Nota: Presione en ejecutar para visualizar documento

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, como 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.

Indicadores de compromiso del archivo adjunto

Nombre del Archivo:	3bfd481026e41ec215bba23c36b8ca25b208ff836fe7b2ca4bea396ad9e83623
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	March 31, 2025 at 17:09:37
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows, 11 sections
MD5:	ead18e0648aa7047895bc4597deb9f77
SHA1:	0be20f709575304de64fc9d792a544c1e4af8b75

SHA256:	3bfd481026e41ec215bba23c36b8ca25b208ff836fe7b2ca4bea396ad9e83623
SSDEEP:	98304:OOY+c3/EsNM917CeeIf1ckg25kKaZWFs0F:OOrc3/1NMyea25buWFs0F

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\<USER>\Desktop\584_6619.exe"	"C:\Users\<USER>\Desktop\584_6619.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

CSIRT Académico UNAD
Correo electrónico: csirt@unad.edu.co
(+57 1) 344 37 00 Ext. 1042516