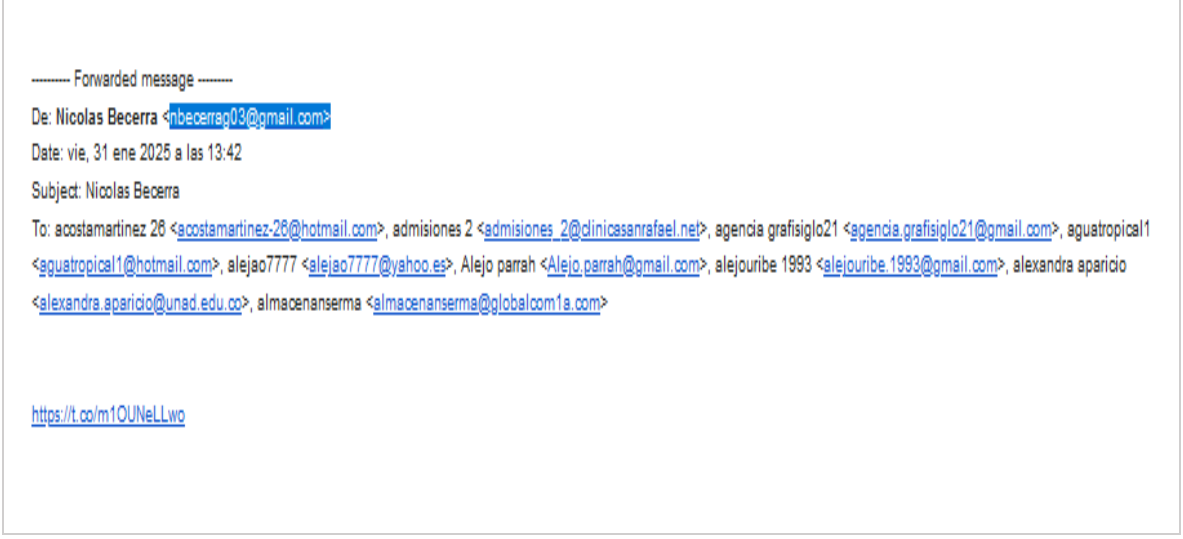
Febrero 03 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.
Cuenta de correo del remitente:	nbecerrag03@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



--------- Forwarded message ---------

De: Nicolas Becerra <nbecerrag03@gmail.com>

Date: vie, 31 ene 2025 a las 13:42

Subject: Nicolas Becerra

To: acostamartinez 26 <acostamartinez-26@hotmail.com>, admisiones 2 <admisiones_2@clinicasanrafael.net>, agencia grafisiglo21 <agencia.grafisiglo21@gmail.com>, aguatropical1 <aguatropical1@hotmail.com>, alejao7777 <alejao7777@yahoo.es>, Alejo parrah <Alejo.parrah@gmail.com>, alejouribe 1993 <alejouribe.1993@gmail.com>, alexandra aparicio <alexandra.aparicio@unad.edu.co>, almacenanserma <almacenanserma@globalcom1a.com>

https://t.co/m1OUNeLLwo

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:	https://t.co/m1OUNeLLwo
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	February 03, 2025 at 15:03:21
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows, 7 sections
MD5:	52A37B5E9EABDDDA2FDF8F069051BD9A
SHA1:	6561609DC81A8C97987FB493AA966783DA67ABE6
SHA256:	9CEA746D950911B0A03444D113085A73F5FD22AC857BE5CC89D6EE77F3BE59D4

SSDEEP:	3:N8DIEwUHSK:28qHSK

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Program Files\Mozilla Firefox\firefox.exe" "https://t.co/m1OUNeLLwo"	"C:\Program Files\Mozilla Firefox\firefox.exe" "https://t.co/m1OUNeLLwo"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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