Marzo 04 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.
Cuenta de correo del remitente:	ie.normalsuperior@medellin.gov.co
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	

De: Institución Educativa Escuela Normal Superior De Medellín <ie.normalsuperior@medellin.gov.co>
Date: vie, 28 feb 2025 a las 10:52
Subject: Seguridad - Verificar Su Correo
To: gloria.gomez@unad.edu.co <gloria.gomez@unad.edu.co>

Agente Microsoft

ENTREGA DE CERTIFICADO DE SU CORREO ELECTRÓNICO

Microsoft

Estimado(a): gloria.gomez@unad.edu.co

Reclamo Microsoft : Codigo :09369 – Verificar su Email

Esto es para informarle que su cuenta de Correo - Email será deshabilitado

ya que ha estado ignorando todos nuestros mensajes para verificar su Correo. Por esta dicha razón será eliminado

Si desea continuar con nuestros servicios, Microsoft por favor verifique su correo dentro de las próximas 24 horas.

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://learned-ionized-learning.glitch.me/
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	March 04, 2025 at 13:52:05
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32+ executable (GUI) x86-64, for MS Windows, 6 sections

MD5:	1AD5D843C48C0309E603561FA21D8E7C
SHA1:	3BCBA3D84708045B05D1F446244957A08C871359
SHA256:	F7A686966A9C9A491C67956D32831C0D3FB27659BCBD2CA6345734366D095B6D
SSDEEP:	3:N8AEc/AEXLZSon:2AEc/A+hn

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "https://learned-ionized-learning.glitch.me/"	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "https://learned-ionized-learning.glitch.me/"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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