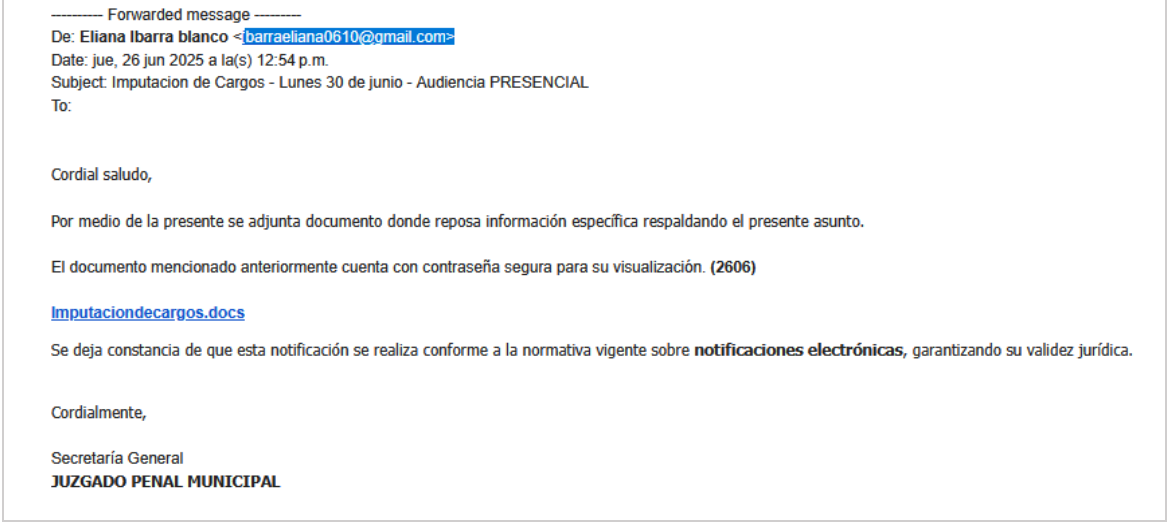
Junio 26 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.valyria
Cuenta de correo del remitente:	barraeliana0610@gmail.com
TLP:	**BLANCO**

Registro grafico relacionado con el Phishing



--------- Forwarded message ---------
De: **Eliana Ibarra blanco** <barraeliana0610@gmail.com>
Date: jue, 26 jun 2025 a la(s) 12:54 p.m.
Subject: Imputacion de Cargos - Lunes 30 de junio - Audiencia PRESENCIAL
To:

Cordial saludo,

Por medio de la presente se adjunta documento donde reposa información específica respaldando el presente asunto.

El documento mencionado anteriormente cuenta con contraseña segura para su visualización. **(2606)**

Imputaciondecargos.docs

Se deja constancia de que esta notificación se realiza conforme a la normativa vigente sobre **notificaciones electrónicas**, garantizando su validez jurídica.

Cordialmente,

Secretaría General
JUZGADO PENAL MUNICIPAL

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:	IMPUT0023-DER-3495830DF348696-23305860390353-230886093424086FFF30854085.VBS
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	June 26, 2025 at 15:39:47
MIME:	text/plain
Información del archivo:	Unicode text, UTF-8 text, with CRLF line terminators
MD5:	4787A10DA890FAAC5B0717FB0638275E
SHA1:	48B2AF011F080D208449CB7268A75B1358C15341

SHA256:	BA68FB1E3C61947D1D0893EF0F2D750CC7B49AE3F97FABEA3BAE60C6EB4AC541
SSDEEP:	768:/4S7EDKhi88EqnG+MmmVJry7DVANZnKlAh7lYVfZZUJgzhOlgt3FTE:/V7GEqnGvBoUUm7lQfZCyNlyVE

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\WINDOWS\System32\OpenWith.exe" C:\Users\admin\AppData\Local\Temp\IMPUT0023-DER-3495830DF348696-23305860390353-230886093424086FFF30854085.VBS.vba	"C:\WINDOWS\System32\OpenWith.exe" C:\Users\admin\AppData\Local\Temp\IMPUT0023-DER-3495830DF348696-23305860390353-230886093424086FFF30854085.VBS.vba	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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