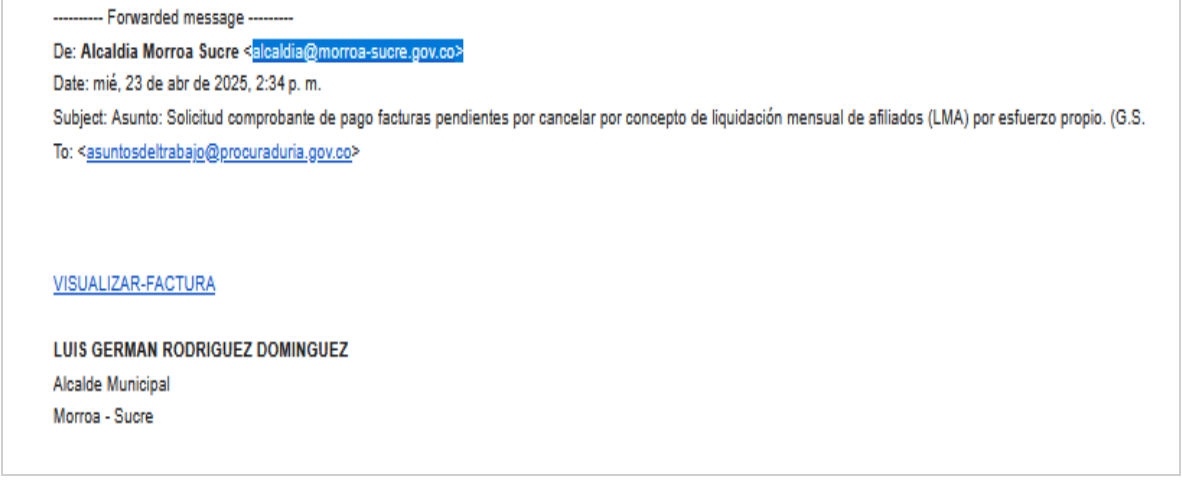
Abril 23 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.tedy/genericrxlo
Cuenta de correo del remitente:	alcaldia@morroa-sucre.gov.co
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



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

De: **Alcaldia Morroa Sucre** <alcaldia@morroa-sucre.gov.co>

Date: mié, 23 de abr de 2025, 2:34 p. m.

Subject: Asunto: Solicitud comprobante de pago facturas pendientes por cancelar por concepto de liquidación mensual de afiliados (LMA) por esfuerzo propio. (G.S.

To: <asuntosdeltrabajo@procuraduria.gov.co>

VISUALIZAR-FACTURA

LUIS GERMAN RODRIGUEZ DOMINGUEZ

Alcalde Municipal

Morroa - Sucre

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:	Comprobante_de_Pago__7122.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	April 23, 2025 at 15:13:01
MIME:	text/plain
Información del archivo:	ASCII text, with very long lines (60231), with CRLF, LF line terminators
MD5:	bfa3416de0d6145bb272e7915375f25a
SHA1:	54149ee89380dfe3cac47538e072c80611eed55f
SHA256:	69242e974eca191b1ac54a0ed754ed3966cd1bcf8b75335b6decbe2449bb4081

SSDEEP:	49152:Ypdbudv7AixBnDu1uv5BG9lmY5tLFXGEwil5E9n3k5SliNi1BG7KQokDqnvtto1G:YpdadD

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\<USER>\Desktop\Comprobante_de_Pago__7122.exe"	"C:\Users\<USER>\Desktop\Comprobante_de_Pago__7122.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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