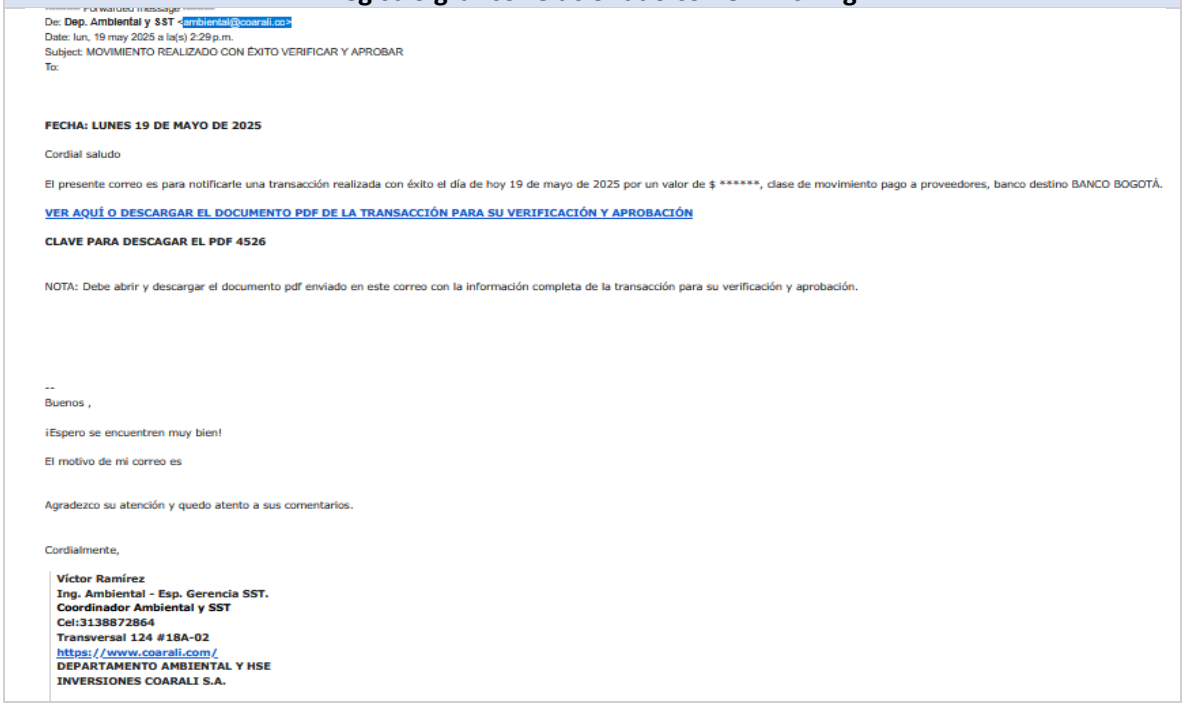
Mayo 19 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	downloader.abxz
Cuenta de correo del remitente:	ambiental@coarali.co
TLP:	**BLANCO**

Registro grafico relacionado con el Phishing



De: **Dep. Ambiental y SST** <ambiental@coarali.co>
Date: lun, 19 may 2025 a la(s) 2:29 p.m.
Subject: MOVIMIENTO REALIZADO CON ÉXITO VERIFICAR Y APROBAR
To:

FECHA: LUNES 19 DE MAYO DE 2025

Cordial saludo

El presente correo es para notificarle una transacción realizada con éxito el día de hoy 19 de mayo de 2025 por un valor de $ ******, clase de movimiento pago a proveedores, banco destino BANCO BOGOTÁ.

VER AQUÍ O DESCARGAR EL DOCUMENTO PDF DE LA TRANSACCIÓN PARA SU VERIFICACIÓN Y APROBACIÓN

CLAVE PARA DESCAGAR EL PDF 4526

NOTA: Debe abrir y descargar el documento pdf enviado en este correo con la información completa de la transacción para su verificación y aprobación.

--
Buenos ,

¡Espero se encuentren muy bien!

El motivo de mi correo es

Agradezco su atención y quedo atento a sus comentarios.

Cordialmente,

Víctor Ramírez
Ing. Ambiental - Esp. Gerencia SST.
Coordinador Ambiental y SST
Cel:3138872864
Transversal 124 #18A-02
https://www.coarali.com/
DEPARTAMENTO AMBIENTAL Y HSE
INVERSIONES COARALI S.A.

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:	DOCUMENTO PDF DE TRANSACCION REALIZADA CON EXITO.vbs
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	May 19, 2025 at 16:48:07

MIME:	text/plain
Información del archivo:	Unicode text, UTF-8 text, with very long lines (449), with CRLF line terminators
MD5:	f8d06e0b3154238e1bd75fa940c517bb
SHA1:	bb0f53cc3c51aadc90840e5b1adf1528243291aa
SHA256:	ca4c2c9cf4320a7f95865a135ec463742ecb3149d174a7d3ee45972f3625e135
SSDEEP:	48:RATcxXtKM6eeaI//aFTeZ8ZZ/O/Y08a8uJ9/O7f5EgsP/+g:RATcxXtKM6eeaI//aFTeZ8ZZ/O/Y08aX

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\WINDOWS\System32\OpenWith.exe" "C:\Users\admin\AppData\Local\Temp\DOCUMENTO PDF DE TRANSACCION REALIZADA CON EXITO.vbs.vba"	"C:\WINDOWS\System32\OpenWith.exe" "C:\Users\admin\AppData\Local\Temp\DOCUMENTO PDF DE TRANSACCION REALIZADA CON EXITO.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