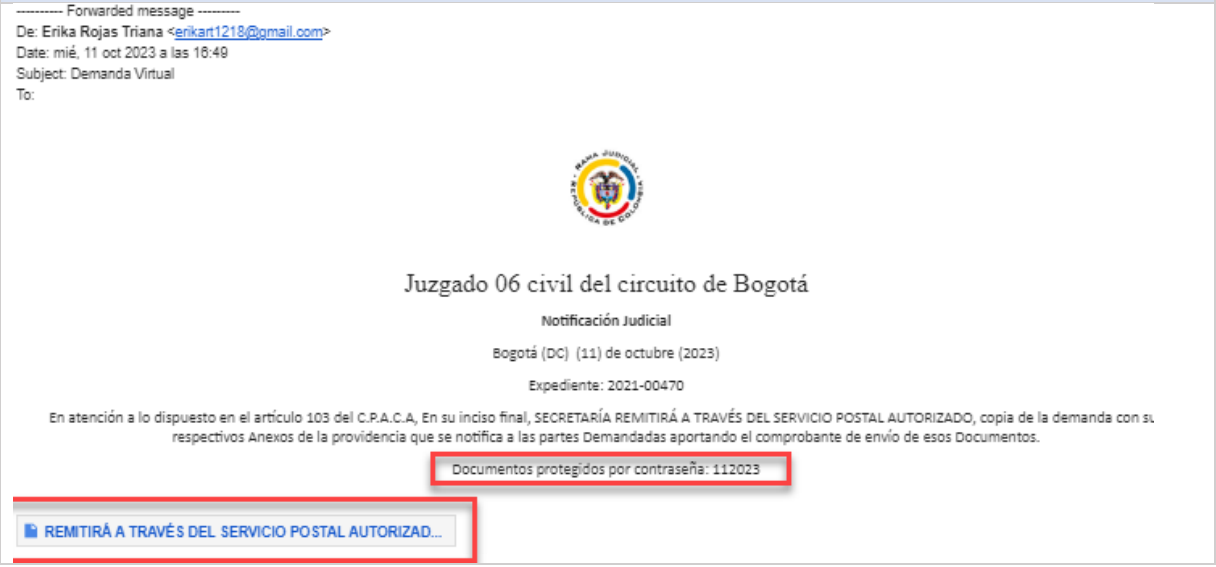
Boletín de Ciberseguridad

Octubre 11 de 2023

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	Sin identificar
Cuenta de correo del remitente:	erikart1218@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



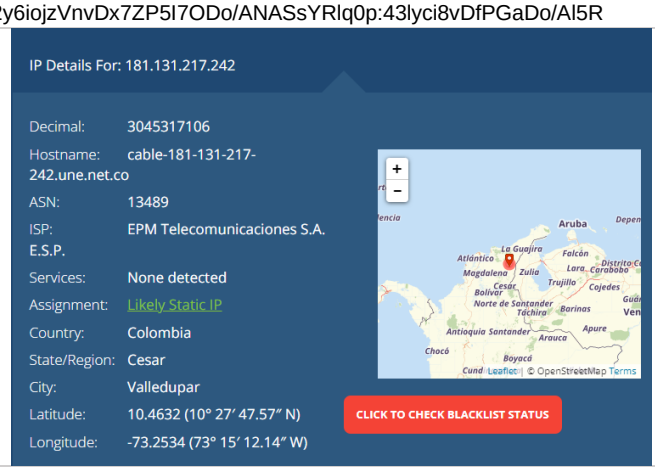
El CSIRT Académico UNAD informa acerca de un asunto de ciberseguridad que ha sido identificado y abordado por este Equipo. Se ha detectado un evento de phishing dirigido a miembros de nuestra comunidad. Es preciso indicar que la técnica de Phishing es un tipo de ataque cibernético en el cual los adversarios intentan engañar a los usuarios para que se revele información confidencial, como contraseñas, números de tarjetas de crédito o información personal.

El archivo adjunto está en capacidad de crear una tarea en el sistema operativo Windows, a partir de comandos VBScript, el cual ejecutaría repetidamente tareas con destino indefinido.

Es preciso aclarar que no es posible realizar el análisis de los procesos secundarios y que se desprenden de la ejecución del archivo, dado que el recurso en el momento del análisis no se encontraba disponible (**http://181.131.217.242/31agosto.vbs**), Es de anotar que en cualquier momento podría ser habilitado el servicio.

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:	REMITIRÁ A TRAVÉS DEL SERVICIO POSTAL AUTORIZADO, copia de la demanda con sus respectivos Anexos_.7z.rEv
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Octubre 11, 2023 at 21:15:00
MIME:	application/x-7z-compressed
Información del archivo:	7-zip archive data, version 0.4
MD5:	FD15BD1D98F5C1DB21833DD27638EE36
SHA1:	1269779FD5326823EEE6325A1AED0F2E9BAA8FDB
SHA256:	D9AEAE3C8426737323DD915F6327B8A89CF17931FD26F124D22E9E814D1CD181
IP/ URL destino	http://181.131.217.242/31agosto.vbs
SSDEEP:	48:43lkrr2y6iojzVnvDx7ZP5I7ODo/ANASsYRlq0p:43lyci8vDfPGaDo/Al5R
Ubicación de la IP	

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Windows\System32\WScript.exe" "C:\Users\admin\Desktop\REMITIRÁ A TRAVÉS DEL SERVICIO POSTAL AUTORIZADO, copia de la demanda con sus respectivos Anexos .wsf"	C:\Windows\System32\wscript.exe	explorer.exe

Se recomienda bloquear dirección IP

Anexo: Archivo con código fuente del malware.

Cordialmente

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