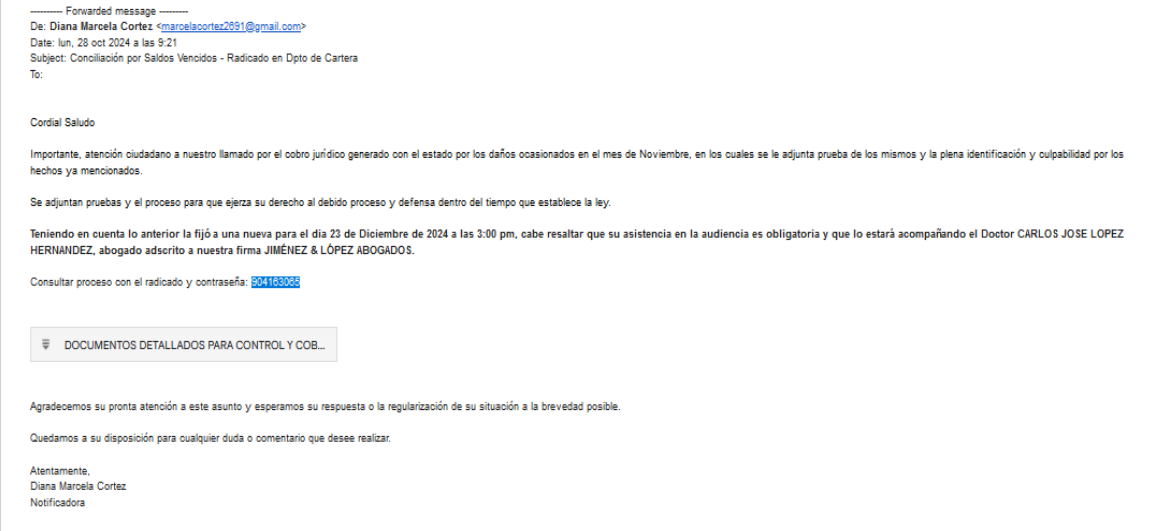
Octubre 29 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.msil/agenttesla
Cuenta de correo del remitente:	marcelacortez2691@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ---------
De: **Diana Marcela Cortez** <marcelacortez2691@gmail.com>
Date: lun, 28 oct 2024 a las 9:21
Subject: Conciliación por Saldos Vencidos - Radicado en Dpto de Cartera
To:

Cordial Saludo

Importante, atención ciudadano a nuestro llamado por el cobro jurídico generado con el estado por los daños ocasionados en el mes de Noviembre, en los cuales se le adjunta prueba de los mismos y la plena identificación y culpabilidad por los hechos ya mencionados.

Se adjuntan pruebas y el proceso para que ejerza su derecho al debido proceso y defensa dentro del tiempo que establece la ley.

Teniendo en cuenta lo anterior la fijó a una nueva para el dia 23 de Diciembre de 2024 a las 3:00 pm, cabe resaltar que su asistencia en la audiencia es obligatoria y que lo estará acompañando el Doctor CARLOS JOSE LOPEZ HERNANDEZ, abogado adscrito a nuestra firma JIMÉNEZ & LÓPEZ ABOGADOS.

Consultar proceso con el radicado y contraseña: 904163065

DOCUMENTOS DETALLADOS PARA CONTROL Y COB...

Agradecemos su pronta atención a este asunto y esperamos su respuesta o la regularización de su situación a la brevedad posible.

Quedamos a su disposición para cualquier duda o comentario que desee realizar.

Atentamente,
Diana Marcela Cortez
Notificadora

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:	DOCUMENTOS DETALLADOS PARA CONTROL Y COBRO, PROCESO LEGAL 98745219541209841623561630254983231041630065 41.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	October 29, 2024 at 11:09:32
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections
MD5:	6431F7984D12C865AEC4CDA803FFFE1A
SHA1:	E34A2CED4F1B0BC8757D1B8C7D0C7461478601B3

SHA256:	3F1C7ADF6A76D7C313BF833CE9D41CD09AD28ECE3C9D56E25A0561D30225C17F
SSDEEP:	49152:wKAAEbreyeTd8Zf2BzQU2OY3Qeca4IpBQXumXi4WDmpBbUCzE2wKfgDG5pn1qz6q:IAEvx+x1JqRD38WDwVU41G2E

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\0f84b3c2-2c6a-4c0c-a9cb-3463394665d3.exe"	"C:\Users\admin\AppData\Local\Temp\0f84b3c2-2c6a-4c0c-a9cb-3463394665d3.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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