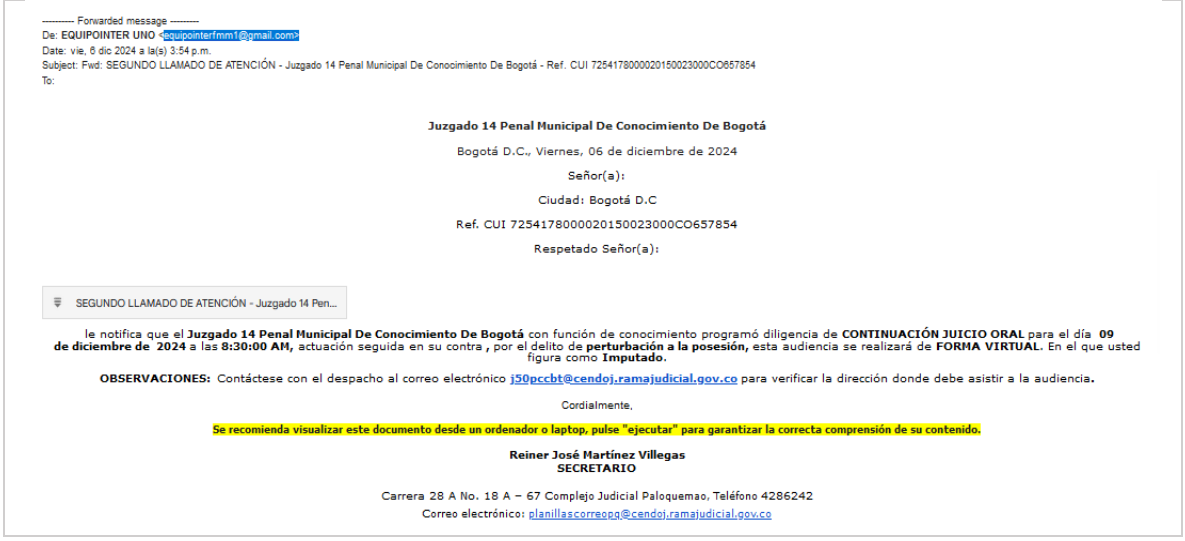
Diciembre 06 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.
Cuenta de correo del remitente:	equipointerfmm1@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ---------
De: **EQUIPOINTER UNO** <equipointerfmm1@gmail.com>
Date: vie, 6 dic 2024 a la(s) 3:54 p.m.
Subject: Fwd: SEGUNDO LLAMADO DE ATENCIÓN - Juzgado 14 Penal Municipal De Conocimiento De Bogotá - Ref. CUI 72541780002015002300OCO657854
To:

Juzgado 14 Penal Municipal De Conocimiento De Bogotá

Bogotá D.C., Viernes, 06 de diciembre de 2024

Señor(a):

Ciudad: Bogotá D.C

Ref. CUI 72541780002015002300OCO657854

Respetado Señor(a):

SEGUNDO LLAMADO DE ATENCIÓN - Juzgado 14 Pen...

le notifica que el **Juzgado 14 Penal Municipal De Conocimiento De Bogotá** con función de conocimiento programó diligencia de **CONTINUACIÓN JUICIO ORAL** para el día **09 de diciembre de 2024** a las **8:30:00 AM,** actuación seguida en su contra , por el delito de **perturbación a la posesión,** esta audiencia se realizará de **FORMA VIRTUAL**. En el que usted figura como **Imputado**.

OBSERVACIONES: Contáctese con el despacho al correo electrónico j50pccbt@cendoj.ramajudicial.gov.co para verificar la dirección donde debe asistir a la audiencia.

Cordialmente,

Se recomienda visualizar este documento desde un ordenador o laptop, pulse "ejecutar" para garantizar la correcta comprensión de su contenido.

Reiner José Martínez Villegas
SECRETARIO

Carrera 28 A No. 18 A – 67 Complejo Judicial Paloquemao, Teléfono 4286242
Correo electrónico: planillascorreopq@cendoj.ramajudicial.gov.co

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.

Se realiza la verificación del archivo en mención, donde:

1. **El archivo no cuenta con ninguna protección mediante contraseña**: Para el usuario final, la ausencia de una contraseña en este tipo de archivos representa un alto riesgo. Al no estar protegido, el archivo puede ser abierto de manera inmediata, aumentando la probabilidad de que el usuario, sin sospechar de su naturaleza maliciosa, lo ejecute. Esto reduce significativamente el tiempo de reacción necesario para identificar la amenaza antes de que cause daño. Además, la facilidad de acceso elimina cualquier barrera

que pudiera obligar al usuario a detenerse y cuestionar la legitimidad del archivo, lo que incrementa el riesgo de infección y exposición de información sensible.

2. **El archivo descargado está comprimido y contiene un acceso directo malicioso**: Al extraer el archivo comprimido, se identificó un acceso directo que aparenta ser archivo legítimo, pero que, al analizar sus propiedades, se observa que es configurado para ejecutar acciones maliciosas. En la pestaña "Documento Web" del acceso directo, se encontró una URL con la siguiente dirección: file://\\77.105.161.126@80\file\AdobeReaderPDF2024.exe

   Esta dirección apunta a un servidor remoto, desde el cual se intenta descargar y posiblemente ejecutar un archivo denominado build.exe. Este comportamiento indica un claro intento de los atacantes de explotar el acceso del usuario para conectarse a un recurso externo y ejecutar un archivo potencialmente malicioso.

   Para el usuario final, este tipo de ataque representa un riesgo crítico porque:

- **Ejecución inadvertida de malware**: El acceso directo puede ser engañosamente presentado como un archivo legítimo, aumentando la probabilidad de que el usuario lo abra sin sospechar de su naturaleza maliciosa.
- **Exposición a servidores maliciosos**: Al intentar acceder a la dirección especificada, el sistema del usuario podría exponer información como la dirección IP o credenciales de red, facilitando un ataque más amplio.
- **Automatización del proceso malicioso**: La configuración del acceso directo permite que la descarga y ejecución del archivo se realice de manera rápida y silenciosa, sin intervención adicional del usuario, reduciendo las posibilidades de detección temprana.

Indicadores de compromiso del archivo adjunto

Nombre del Archivo:	SEGUNDO LLAMADO DE ATENCIÓN - Juzgado 14 Penal Municipal De Conocimiento De Bogotá - Ref. CUI 72541780000201500230000CO657854_zip.rev
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	December 06, 2024 at 19:13:54
MIME:	application/x-rar
Información del archivo:	RAR archive data, v5
MD5:	4B21FF773582358AFC0B3871E8F4F162
SHA1:	9231F2A5A4828997914D57A8A342DC47BEED2EAC
SHA256:	4BAECA0206EFBAC721AD7288F25E7BC26982CC5C1DDB990E1FB359A2E07784EC
SSDEEP:	24:0D5WXWzm1cc5CR8Yy213Gu6u2StO6+wXWzewxby0aftd3KDHKASo4qyrIJnnk XWt:07+Q8Iz6YO6+LJsD3KTd4q+IJnv5

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Program Files\WinRAR\WinRAR.exe" C:\Users\admin\AppData\Local\Temp\17f3056d-8b66-41f6-9c8a-02c812e26584.rar	"C:\Program Files\WinRAR\WinRAR.exe" C:\Users\admin\AppData\Local\Temp\17f3056d-8b66-41f6-9c8a-02c812e26584.rar	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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