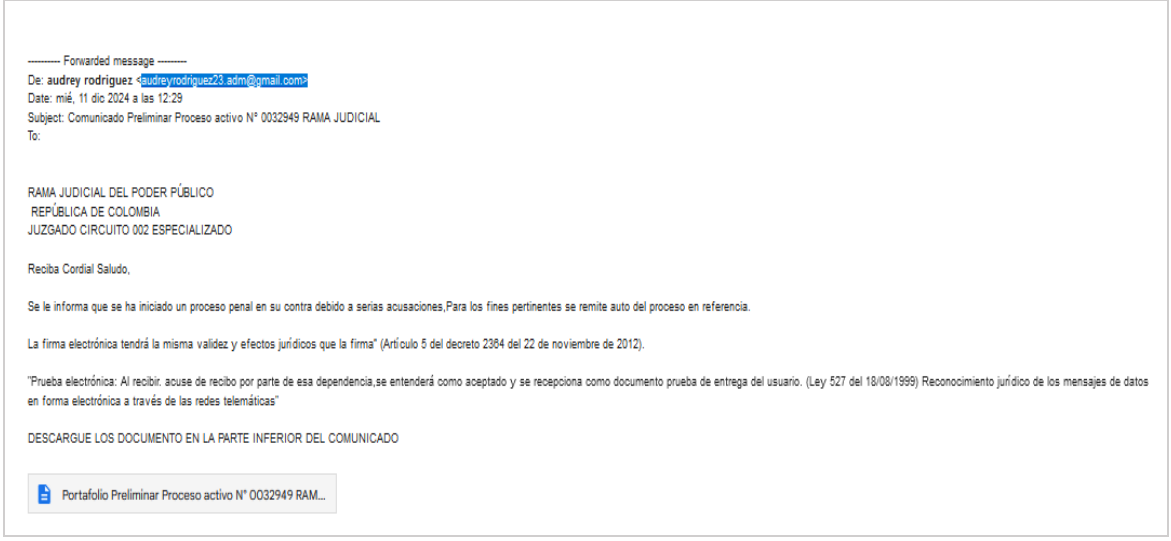
Diciembre 12 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.
Cuenta de correo del remitente:	audreyrodriguez23.adm@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ---------
De: **audrey rodriguez** <audreyrodriguez23.adm@gmail.com>
Date: mié, 11 dic 2024 a las 12:29
Subject: Comunicado Preliminar Proceso activo N° 0032949 RAMA JUDICIAL
To:

RAMA JUDICIAL DEL PODER PÚBLICO
REPÚBLICA DE COLOMBIA
JUZGADO CIRCUITO 002 ESPECIALIZADO

Reciba Cordial Saludo,

Se le informa que se ha iniciado un proceso penal en su contra debido a serias acusaciones,Para los fines pertinentes se remite auto del proceso en referencia.

La firma electrónica tendrá la misma validez y efectos jurídicos que la firma" (Artículo 5 del decreto 2364 del 22 de noviembre de 2012).

"Prueba electrónica: Al recibir. acuse de recibo por parte de esa dependencia,se entenderá como aceptado y se recepciona como documento prueba de entrega del usuario. (Ley 527 del 18/08/1999) Reconocimiento jurídico de los mensajes de datos en forma electrónica a través de las redes telemáticas"

DESCARGUE LOS DOCUMENTO EN LA PARTE INFERIOR DEL COMUNICADO

Portafolio Preliminar Proceso activo N° 0032949 RAM...

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://\\62.60.226.24@80\file\PDFReader.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:	Portafolio Preliminar Proceso activo N° 0032949 RAMA JUDICIAL.url
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	December 12, 2024 at 11:33:47
MIME:	application/x-wine-extension-ini
Información del archivo:	Generic INItialization configuration [InternetShortcut]
MD5:	FF05EADEB00D00F01BFBB29AB7B74B2E
SHA1:	2C64637BE98C0DEE4759A2BC6ED30D7AE7ABA8A7
SHA256:	A69C825854983C417970BAEA932318010672CB836C6F6721577657D1DDB530E7
SSDEEP:	6:JyXSvVG/FTVmJtOFJblvstXbPAbhYNrIEirQsv:cXaVWfmJtOFJB0tLjS

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\WINDOWS\system32\rundll32.exe" "C:\WINDOWS\system32\ieframe.dll",OpenURL %l	"C:\WINDOWS\system32\rundll32.exe" "C:\WINDOWS\system32\ieframe.dll",OpenURL %l	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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