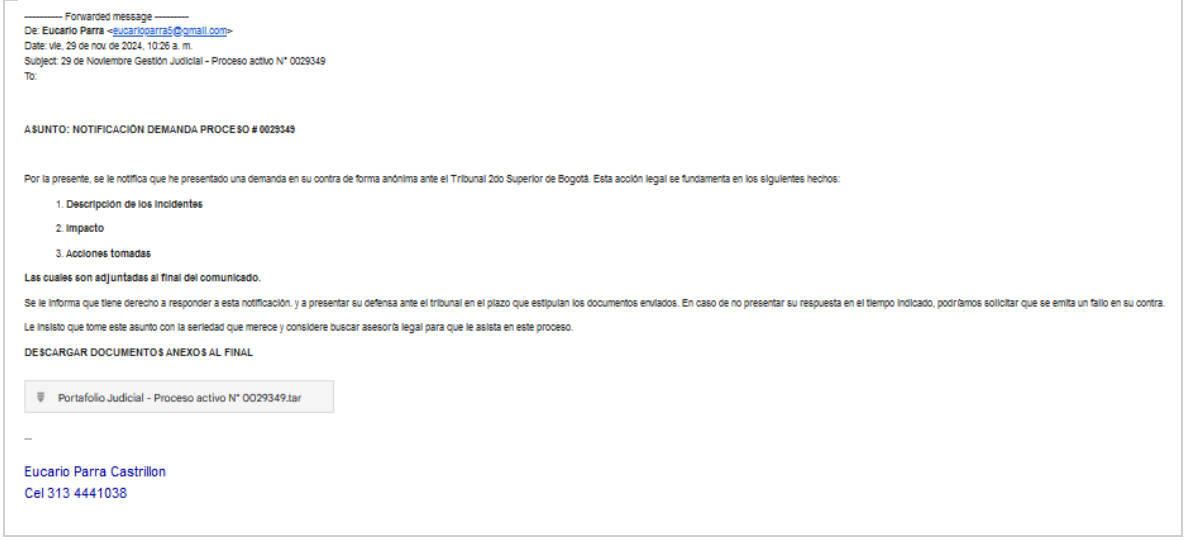
Noviembre 29 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.loader
Cuenta de correo del remitente:	eucarioparra5@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ---------
De: **Eucario Parra** <eucarioparra5@gmail.com>
Date: vie, 29 de nov de 2024, 10:26 a. m.
Subject: 29 de Noviembre Gestión Judicial - Proceso activo N° 0029349
To:

ASUNTO: NOTIFICACIÓN DEMANDA PROCESO # 0029349

Por la presente, se le notifica que he presentado una demanda en su contra de forma anónima ante el Tribunal 2do Superior de Bogotá. Esta acción legal se fundamenta en los siguientes hechos:

1. **Descripción de los incidentes**
2. **Impacto**
3. **Acciones tomadas**

Las cuales son adjuntadas al final del comunicado.

Se le informa que tiene derecho a responder a esta notificación. y a presentar su defensa ante el tribunal en el plazo que estipulan los documentos enviados. En caso de no presentar su respuesta en el tiempo indicado, podríamos solicitar que se emita un fallo en su contra.

Le insisto que tome este asunto con la seriedad que merece y considere buscar asesoría legal para que le asista en este proceso.

DESCARGAR DOCUMENTOS ANEXOS AL FINAL

Portafolio Judicial - Proceso activo N° 0029349.tar

--

Eucario Parra Castrillon
Cel 313 4441038

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 un archivo legítimo, pero que, al analizar sus propiedades, se observó que está configurado para ejecutar una acción maliciosa. En la pestaña "Documento Web" del acceso directo, se encontró una URL con la siguiente dirección: file://\\77.105.161.126@80\file\build.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:	build.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	November 29, 2024 at 12:02:38
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows, 7 sections
MD5:	2C4B3F00FF2A1958E4D390DEDB626F52
SHA1:	EEB0426A770708432F94D47F2FD9E4525EF7A090
SHA256:	CE7792FF95DCA6CD5B06083ACEFC42D131AAE24000A4FC1C67DA24F083DA9C6A
SSDEEP:	98304:kYnBJ6zfr244vkagwa0R1Loj/V3nLnfCttOQ/tT/EDos+lp0TOkZVdoVuayNmNi0:wjrgp

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\build.exe"	"C:\Users\admin\AppData\Local\Temp\build.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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