Informe

Técnico

Malware de la Semana

COLCERT IN-20250530-022

TLP:CLEAR

Consejo Superior de la Judicatura
Dirección Seccional de Administración Judicial de Bogotá

Bogotá 21 de mayo del 2025

RAMA JUDICIAL - REPÚBLICA DE COLOMBIA
CONSEJO SUPERIOR DE LA JUDICATURA

ESTIMADO:
DEMANDADO.

RADICADO CUI: 20259969-9966569-99962366-9986

Asunto: Citación judicial obligatoria – proceso por falsedad en documento público y cohecho.

Por medio de la presente, el Despacho Jurídico Penal No. 12 de Bogotá D.C. le notifica que ha sido citado(a) en calidad de indiciado, en el proceso penal radicado bajo el número 20259969-9966569-99962366-9986, por su presunta participación en los delitos de:

Durante la semana anterior, el ColCERT ha detectado una campaña maliciosa que explota la ingeniería social, **haciéndose pasar por entidades oficiales del Estado colombiano.** Esta campaña entrega un archivo .zip protegido con contraseña que simula una citación judicial, cuyo contenido real es un **ejecutable malicioso que despliega HijackLoader,** un malware modular usado para el despliegue de payloads adicionales como stealers, RATs y ransomware.

Información Técnica de la Muestra

- **Nombre del archivo: 1Detalles diligencia judicial.exe**
- **Tamaño:** 70 KB
- **Tipo:**PE32+ executable (console) x86-64
- **Análisis dinámico:**Trellix IVX Cloud Sandbox
- **Resultado:Malicioso**
- **Procesos observados:**rundll32.exe (invocado ≥60 veces desde %TEMP%)
- **Acciones clave:**Carga modular de DLLs, ejecución reflexiva, evasión de VM
- **Persistencia:**HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- **Perfiles utilizados:**win10x64n, win7x64e, win10x64p

Identificadores de Hash (IoC)

Tipo	Valor
MD5	7d6a19f1e84d6bc9e23b1fd3c8f6ab4e
SHA1	1f2e6fce5ecb1aa63fd7cc63062c2a680a7d7a3
SHA256 (.exe)	2b2f414a6619442e0f58cefe115ec1cc7cd6729e9d91ab1e7e4af063b686ce91
SHA256 (.zip)	07005d9489e6771aca9a58e6f5760cd513980ffeb04f909850c6cfd5f04dd2ef
SHA256 (.bin)	07005d9489e6771aca9a58e6f5760cd513980ffeb04f909850c6cfd5f04dd2ef (idéntico al .zip)

URLs Maliciosas Completas

Redireccionador desde correo

hxxps[:]//nts[.]embluemail[.]com/p/cl?s=I0wegKXsPnaBDu-znl_o82YZmfYjGbm5&data=QQnQlLMo%2FL89E9q%2FY%2FUKbhYE8a2BO1gccVCuTAb5NGZPe6rt%2F1GpH7%2FybLtiVQ7KtLkny1Tcrmi2noYx8KQ5f7yEtq0EiSfBzBGRrMp%2F9bI%3D!-!af6cna!-!hxxps%3A%2F%2Fu[.]pcloud[.]link%2Fpublink%2Fshow%3Fcode%3DXZtpUh5ZAy1FyGpBOp7b6AxdjTW5yF6hc3ry%26utm_source=emBlue%26utm_medium=email%26utm_campaign=PROCESO+INFORMATIVO%26utm_content=INFORMES+2025--Citaci%C3%B3n+oficial+a+diligencia+judicial+%E2%80%93+Proceso+penal+activo+Bogot%C3%A1+D[.]C[.]%26utm_term=multiple--3--none--0-10--ENVIO+SIMPLE&t=aHR0cHM6Ly91LnBjbG91ZC5saW5rL3B1Ymxpbmsvc2hvdw==

URL final (descarga directa desde pCloud)

hxxps[:]//u[.]pcloud[.]link/publink/show?code=XZtpUh5ZAy1FyGpBOp7b6AxdjTW5yF6hc3ry&utm_source=emBlue&utm_medium=email&utm_campaign=PROCESO+INFORMATIVO&utm_content=INFORMES+2025--Citaci%C3%B3n+oficial+a+diligencia+judicial+–+Proceso+penal+activo+Bogot%C3%A1+D[.]C[.]&utm_term=multiple--3--none--0-10--ENVIO+SIMPLE

Técnicas MITRE ATT&CK Observadas

Fase	Técnica ID	Aplicación del malware	Descripción y evidencia del caso
Ejecución	T1055.003	rundll32.exe carga módulos cifrados en cadena	El ejecutable principal lanza más de **60 instancias de rundll32.exe** con DLLs externas como libnettle-8.dll. Esto refleja un patrón de **inyección de código y ejecución por etapas**.
Persistencia	T1547.001	Registro HKCU\Software\Microsoft\Windows\CurrentVersion\Run	El análisis dinámico mostró que la muestra **modifica claves de ejecución automática**, asegurando que el malware se inicie tras reinicios del sistema. Se confirmó entrada persistente en el hive HKCU.
Evasión	T1497 / T1027	Anti-VM / packing y ejecución modular cifrada	La muestra emplea **compresión ZIP con método no soportado**, ocultamiento de carga (sospechoso.bin) y múltiples DLLs. No ejecuta bien en sandboxes estándar (evidencia: errores en entornos controlados).
Descubrimiento	T1082	Uso de WMI para obtener sistema, red y memoria	El comportamiento observado incluye **consulta de entorno** (procesos, versión de sistema y perfil del host). Esto indica que el malware verifica si se encuentra en un entorno válido antes de actuar.
C2	T1071.001	Comunicación HTTPS con dominios legítimos	Aunque no se detectó tráfico directo a C2 custom, sí se observó tráfico HTTPS hacia dominios legítimos como outlook.live.com y digicert.com, lo que sugiere **uso de canales encubiertos de comunicación**.

Análisis de Evidencia - Parrot OS

Se utilizó el siguiente entorno y herramientas para el análisis:

Entorno: Máquina virtual con Parrot OS
Herramientas7z, file, sha256sum, mv, cp, strings, peframe, bash

Pasos realizados:

- ❑ Extracción del ZIP protegido con 7z
- ❑ Renombrado seguro a sospechoso.bin
- ❑ Validación del tipo de archivo con file
- ❑ Cálculo de hash SHA256
- ❑ Análisis de cadenas con strings
- ❑ Automatización con script personalizado
- ❑ Inspección estática tentativa con peframe

Etapa	Acción ejecutada
Descarga	Archivo zip desde pCloud
Clave	citacion2025
Método	Se usó 7z debido a compresión no soportada (method 99)
Extraído	.zip interno → ejecutable disfrazado
Renombrado	Se renombró a sospechoso.bin para análisis seguro
Descompresión final	Se extrajo 1Detalles diligencia judicial.exe

HijackLoader es un malware tipo loader modular diseñado para ejecutar en memoria código malicioso de forma ofuscada y en múltiples etapas.

Su principal función es servir de puente para cargar otros tipos de malware (como stealers, RATs o ransomware), utilizando técnicas de evasión como inyección en procesos legítimos (rundll32.exe), persistencia en el registro, y comunicación cifrada con infraestructura de comando y control (C2).

Es altamente silencioso y evasivo, dificultando su detección por soluciones tradicionales.

COLCERT

Proceso de análisis manual en Parrot OS

Validación y extracción del ejecutable:

- 7z x "Citación Judicial.zip" -p"citacion2025" –y
- mv 'DETALLES ... .zip' sospechoso.bin
- 7z x sospechoso.bin

Inspección:

- file 1Detalles\ diligencia\ judicial.exe
- sha256sum 1Detalles\ diligencia\ judicial.exe
- strings 1Detalles\ diligencia\ judicial.exe | grep -i 'dll\|http'

Se confirmaron strings relacionadas con certificados DigiCert, DLLs externas y referencias de ejecución por etapas.

Resultado sandbox (Detectic.colcert.gov.co)

Acciones detectadas:

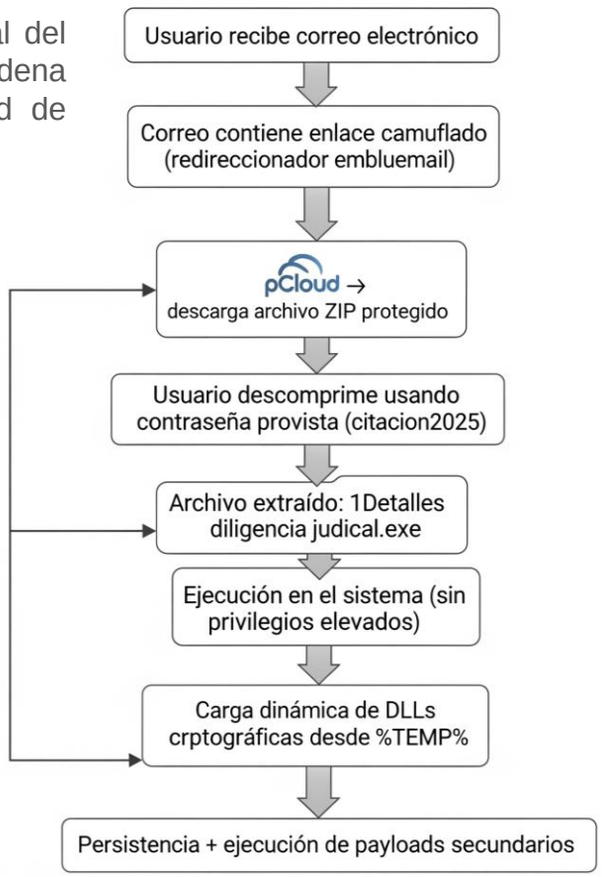
- **Clasificación:** Malicioso
- **Tipo de ejecución:** Loader en consola con ejecución en memoria
- **Comportamientos clave:**
  - Uso de rundll32.exe como cargador en cadena de módulos
  - Persistencia mediante clave de registro Run (HKCU\...\Run)
  - Tráfico HTTPS hacia dominios legítimos (canales C2 encubiertos)
  - Técnicas de evasión de sandbox y entornos virtuales
  - Conexiones a:
    - *outlook.live.com*
    - *mozaws.net*
    - *digicert.com (legítimos, utilizados como canal de control)*

Vector de Ataque (Gráfico)

La imagen ilustra el vector de ataque completo, desde la entrega inicial del malware hasta la ejecución de payloads secundarios. Se observa una cadena estructurada de ingeniería social, descarga y ejecución sin necesidad de privilegios elevados, seguida de técnicas de evasión y persistencia.

Los pasos clave son:

1.Correo malicioso: El usuario recibe un mensaje suplantando una citación judicial.
2.Redireccionador: El enlace contenido en el correo utiliza un dominio legítimo (embluemail.com) como camuflaje.
3. **Descarga:** El usuario accede a un archivo .zip alojado en pCloud, protegido con contraseña (citacion2025).
4.Descompresión y ejecución: Se extrae un ejecutable disfrazado (1Detalles diligencia judicial.exe), que el usuario ejecuta sin saberlo.
5.Carga dinámica de DLLs: Se despliega código malicioso usando rundll32.exe para cargar DLLs desde %TEMP%.
6.Persistencia y payloads adicionales: El malware establece persistencia y queda listo para desplegar módulos adicionales (como stealers o ransomware).



COLCERT

Recomendaciones Técnicas de Mitigación

Las siguientes acciones están diseñadas para mitigar los vectores utilizados por esta amenaza (HijackLoader), reducir la exposición y detectar su comportamiento en entornos corporativos o gubernamentales:

1 A nivel de Red / Proxy / Firewall

Bloquear o colocar en lista gris los siguientes dominios:

- ❑ pcloud.link
- ❑ nts.embluemail.com

- ❑ Inspeccionar tráfico HTTPS saliente hacia dominios legítimos con inspección SSL profunda (SSL inspection / TLS decryption).
- ❑ Activar alertas sobre User-Agent anómalos o personalizados en solicitudes salientes.
- ❑ Aplicar reglas de filtrado para prevenir descarga de archivos comprimidos .zip desde dominios no aprobados.

2 A nivel de endpoint

- ❑ Restringir ejecución de rundll32.exe desde ubicaciones no estándar, como %TEMP%, %APPDATA% o subdirectorios ocultos.
- ❑ Bloquear ejecución de archivos .exe extraídos desde archivos .zip con contraseña (vía GPO o reglas de EDR).
- ❑ Habilitar detección de ejecución en consola (PE32+ console) para procesos anómalos que no usan interfaz gráfica.
- ❑ Monitorear escritura en claves de registro persistente, como:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
```

- ❑ Aislar procesos de rundll32.exe que lancen múltiples instancias en cadena o carguen DLLs externas.

3 A nivel de Usuario / Concienciación

- ❑ Realizar campañas de phishing simulado usando ejemplos reales como citaciones judiciales para educar sobre el riesgo.
- ❑ Capacitar al personal sobre los riesgos de abrir ZIPs con contraseña recibidos por correo.
- ❑ Reforzar que ninguna entidad oficial del Estado colombiano envía archivos protegidos con clave por canales no autenticados.

4 A nivel de SOC / Detección avanzada

Implementar reglas YARA para detectar cargas PE con:

- ❑ Uso de DLLs criptográficas externas (libgmp, libnettle).
- ❑ Strings relacionadas con rundll32.exe y ejecución en consola.
- ❑ Usar EDR para alertar sobre comportamientos de proceso reflejados (process hollowing, DLL side-loading).
- ❑ Correlacionar eventos relacionados con ejecución de binarios desde ZIP protegidos.

5 Otras medidas complementarias

- ❑ Desactivar ejecución automática de archivos desde unidades extraíbles o directorios temporales.
- ❑ Activar AppLocker o Windows Defender Application Control (WDAC) para bloquear cargas no firmadas.
- ❑ Auditar presencia de las siguientes DLLs:
- ❑ libgmp-10.dll, libhogweed-6.dll, libnettle-8.dll

Herramientas de Análisis Utilizadas

- **Sistema operativo:** Parrot OS Security Edition (VM)
- **Consola:** bash
- **Extracción:** 7z (soporte para método de compresión 99 + contraseña)
- **Validación binaria:** file, sha256sum, md5sum, sha1sum
- **Inspección:** strings (detección de artefactos ocultos, rutas, DLLs)
- **Scripts** personalizados en bash
- **Análisis estático:** peframe (uso limitado por dependencias)
- **Sandbox:** Trellix IVX Cloud (detección de comportamiento en memoria)
- **Navegador manual con protección** (uso de navegador aislado para URL tracking)

Fuentes Oficiales

- **MITRE ATT&CK Framework** - https://attack.mitre.org
- **Trellix (McAfee) Sandbox Analysis -** https://www.trellix.com
- **pCloud Legal Policy –** Revisión **del servicio usado para alojar malware -** https://www.pcloud.com/legal-terms-of-service.html
- **Microsoft OCSP/DigiCert Trust Anchors – Dominios legítimos utilizados para camuflar tráfico C2 -** https://www.digicert.com/digicert-root-certificates.htm
- **COLCERT – Lineamientos de ciberseguridad – Referencia nacional para alertas y manejo de incidentes -** https://colcert.gov.co/800/w3-channel.html