Cuando trabajamos con NTFS, cada archivo puede contener varios “flujos” de datos. El contenido normal del archivo es solo uno de ellos. Podemos agregar flujos adicionales con cualquier nombre, y estos **no aparecen en el Explorador de archivos**, ni modifican el tamaño del archivo principal que vemos en las propiedades.

En pentesting y análisis forense, los ADS (Alternate Data Stream) son especialmente interesantes porque permiten esconder datos, payloads o información sensible sin alterar el archivo visible que se ve a simple vista.

Creando un ADS con Notepad

Si ejecutamos el siguiente comando en una consola de Windows:

```
notepad archivo.txt:hidden
```

Windows no abre directamente el archivo archivo.txt, sino un **stream alternativo** llamado hidden. Si ese flujo no existe, Notepad lo crea. Si ya existe, lo abre sin mostrar nada del contenido principal del archivo. El archivo principal puede pesar, por ejemplo, 1 KB, pero el ADS puede contener 100 MB, y nadie lo verá simplemente mirando las propiedades del archivo.

Escribiendo directamente en un ADS

También podemos escribir contenido dentro de un ADS desde la línea de comandos, sin tocar el contenido visible del archivo:

```
echo Esto está oculto > archivo.txt:hidden
```

El contenido de archivo.txt no cambia. Todo el texto se guarda en el flujo alternativo hidden, que queda oculto para la mayoría de las aplicaciones y del propio Explorador de archivos.

Leyendo el contenido de un ADS

Para leer el contenido de un ADS, podemos usar:

```
more < archivo.txt:hidden
```

o también:

```
type archivo.txt:hidden
```

En ambos casos estamos accediendo al flujo alternativo, no al contenido principal del archivo.

Detectando ADS en un sistema Windows

Windows no lista los ADS de forma normal. Si queremos ver los streams alternativos asociados a archivos en un directorio, tenemos que usar:

```
dir /r
```

Este comando nos muestra los flujos alternativos de datos asociados a cada archivo. Aun así, muchas herramientas de backup, antivirus y monitores de integridad **ignoran los ADS**, por lo que su detección no siempre es trivial.

También podemos usar el comando **streams**.

Borrando un ADS

Si queremos eliminar un stream alternativo concreto, podemos hacerlo de forma directa:

```
del archivo.txt:hidden
```

Otra opción es vaciarlo para dejarlo sin contenido:

```
type nul > archivo.txt:hidden
```

En ambos casos actuamos solo sobre el flujo alternativo, sin eliminar el archivo principal.

Relevancia de los ADS en ciberseguridad

Desde el punto de vista de la ciberseguridad, los ADS son útiles para:

- Ocultar payloads o configuraciones sin generar sospechas evidentes.
- Almacenar datos exfiltrados temporalmente antes de cifrarlos o moverlos.
- Probar técnicas básicas de evasión frente a herramientas que solo inspeccionan el contenido principal de los archivos.

Desde el lado del análisis forense y de las auditorías, revisar la presencia de ADS es obligatorio cuando auditamos sistemas Windows, especialmente si investigamos mecanismos de persistencia o formas de almacenamiento encubierto utilizadas por malware o atacantes.

Como conclusión, los Alternate Data Streams no son un fallo de seguridad en sí mismos, sino una funcionalidad de NTFS que, si no se conoce y no se monitoriza, se puede convertir en una vía de ocultación muy cómoda para quien quiere esconder información en un sistema comprometido.