Introduction to Alternate Data Streams | Malwarebytes Labs

By Pieter Arntz

Published: 2015-07-21 · Archived: 2026-04-05 13:16:15 UTC

What are Alternate Data Streams?

Alternate Data Streams (ADS) are a file attribute only found on the NTFS file system.

In this system a file is built up from a couple of attributes, one of them is *$Data*, aka the data attribute. Looking at the regular data stream of a text file there is no mystery. It simply contains the text inside the text file. But that is only the primary data stream.

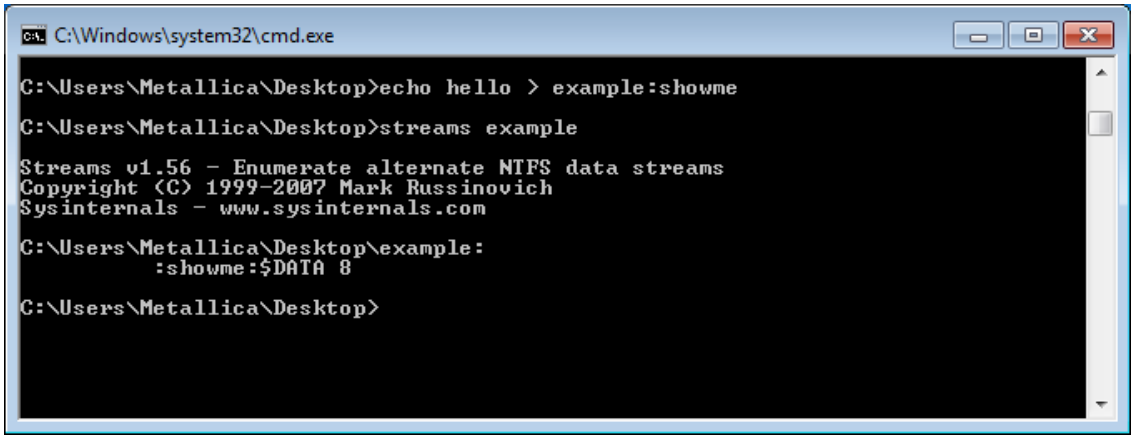
This one is sometimes referred to as the unnamed data stream since the name string of this attribute is empty (“”) . So any data stream that has a name is considered alternate.

These data streams suffer from a bad reputation since they have been used and abused to write hidden data. Varying from data about where a file came from to complete malware files (e.g. Backdoor.Rustock.A)

If you are up for an experiment, we can easily create and read an alternate data stream.

Streams

The first tool you can use was developed by Sysinternals (later bought by Microsoft) and is called Streams *(nomen est omen)*.



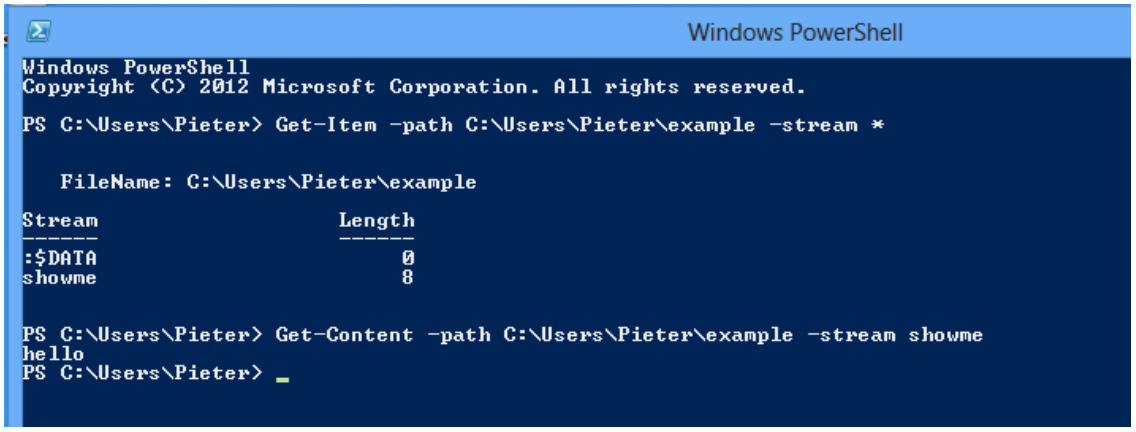
In the example above we used the echo command to create an empty file called example with an alternate data stream called showme.

By using streams we can check which files have alternate data-streams. In the results visible in the above command prompt, *$Data* is the name of the attribute (as discussed earlier) and the 8 tells us the size.

But since we are looking at it, we obviously would like to see what is inside the alternate data streams. Unfortunately, streams do not offer that option.

Get-Item

If you are using Windows 8 (or newer) there is a built-in option to read ADS. You can use PowerShell commands to achieve this. For those that have no experience with it, you can start it by typing PowerShell in the Run box (Windows key + R) and follow the lines in this screenshot.

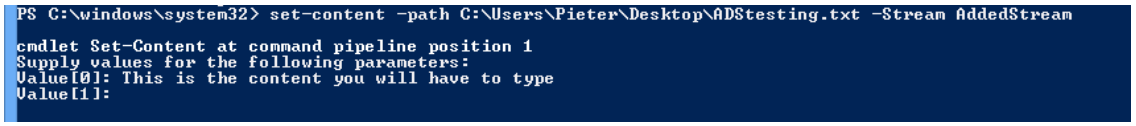


Set-item

Another thing that you can do with Powershell is add streams to a file. The Powershell command syntax is:

```
set-content - path {path to the file} - stream {name of the stream}
```

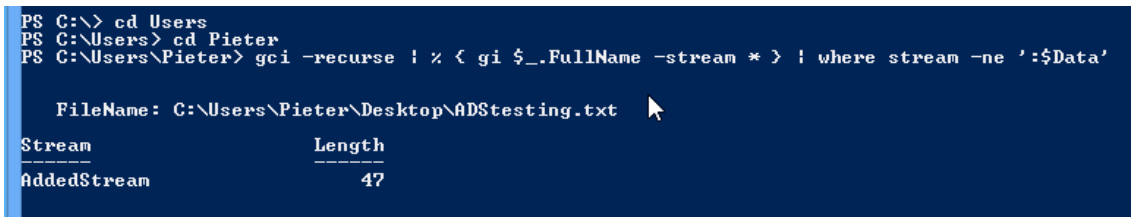
Doing so will initiate a cmdlet where you can enter the content of the stream under Value[i]



Search for ADS

If you want to search a directory or drive for ADS you can use this command in the root of the target:

```
gci -recurse | % { gi $_.FullName -stream * } | where stream -ne ':$Data'
```



Be warned that if you include the Windows directory in your search you will likely receive an enormous list.

Remove ADS

A word of warning here. Removing ADS is not always advisable. Some of them are needed for the proper use of the software that created the streams. So make sure you have done your research before removing them. The syntax is:

```
remove-item -path {path to the file} -stream {name of the stream}
```

Malwarebytes Anti-Malware scans for and removes unwanted ADS (as Rootkit.ADS)

Summary

Alternate Data Streams (ADS) have been given a bad reputation because their capability to hide data from us on our own computer, has been abused by malware writers in the past. Hopefully this article will clear up some of the questions and mystique you had about ADS.

Resources:

- Alternate data streams in NTFS
- Exploring Alternate Data Streams

About the author

Was a Microsoft MVP in consumer security for 12 years running. Can speak four languages. Smells of rich mahogany and leather-bound books.
