ODDVAR MOE'S BLOG

Notes from My adventures with Windows security

PUTTING DATA IN ALTERNATE DATA STREAMS AND HOW TO EXECUTE IT – PART 2

Posted on 11 Apr 2018

I wrote a blogpost a while back about Alternate data streams that you can find here: https://oddvar.moe/2018/01/14/putting-data-in-alternate-data-streams-and-how-to-execute-it/

After I wrote that post I have made some new discoveries that I wanted to share around Alternate data streams. As you probably already know if you read some of my stuff is that I am a big fan of Living off the land techniques.

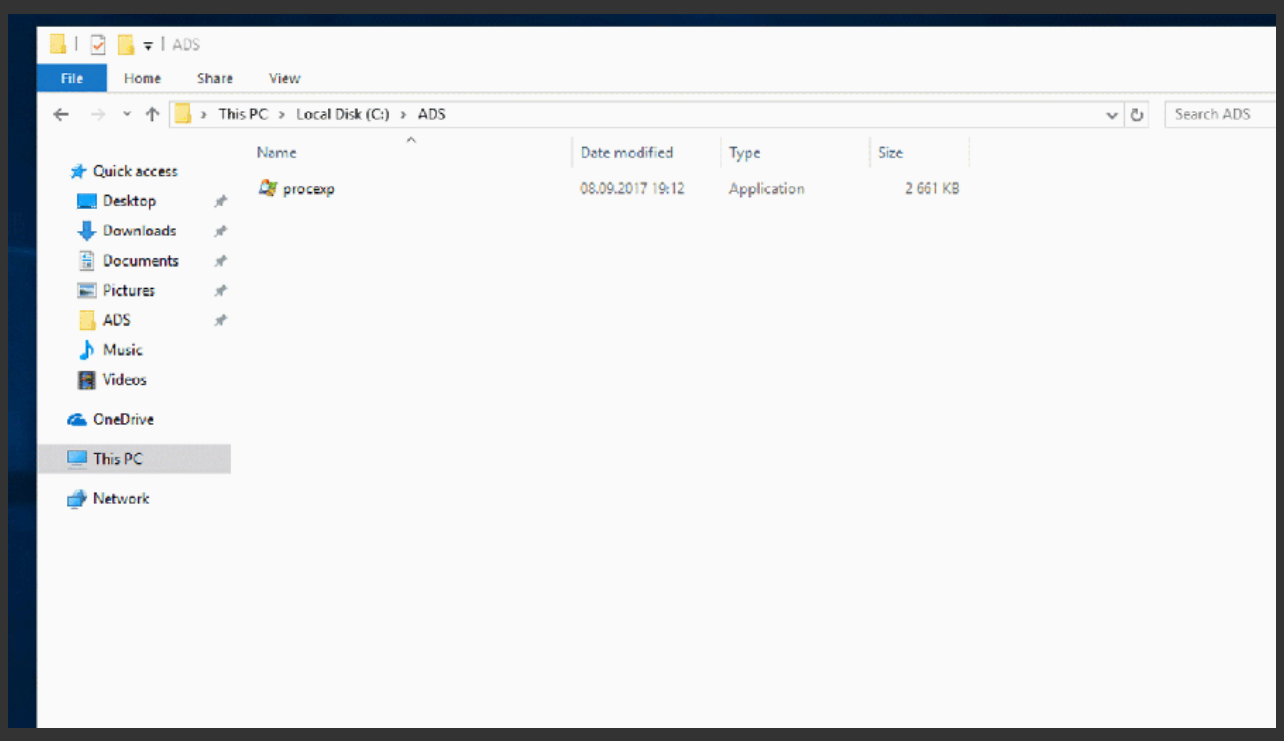
The only method I knew about to inject data into a alternate data stream when I wrote the first post was the "type" command.
I have since my last blogpost discovered some other techniques as well. These techniques I have discovered can of course have been discovered by others and already been blogged about, if so please let me know and I will link to your blogpost.

EXTRAC32.EXE

First up is extrac32. If do not know this command you can read more about it here: https://ss64.com/nt/extract.html

Basically what you use it for is to extract cab files. What I figured out was that you also can use this command to add alternate data streams. The PoC for doing this (including creating a CAB) looks like this:

```
echo "empty file" > c:\ADS\file.txt
makecab c:\ADS\procexp.exe c:\ADS\procexp.cab
extrac32 C:\ADS\procexp.cab c:\ADS\file.txt:procexp.exe
wmic process call create '"c:\ADS\file.txt:procexp.exe"'
```



FINDSTR.EXE

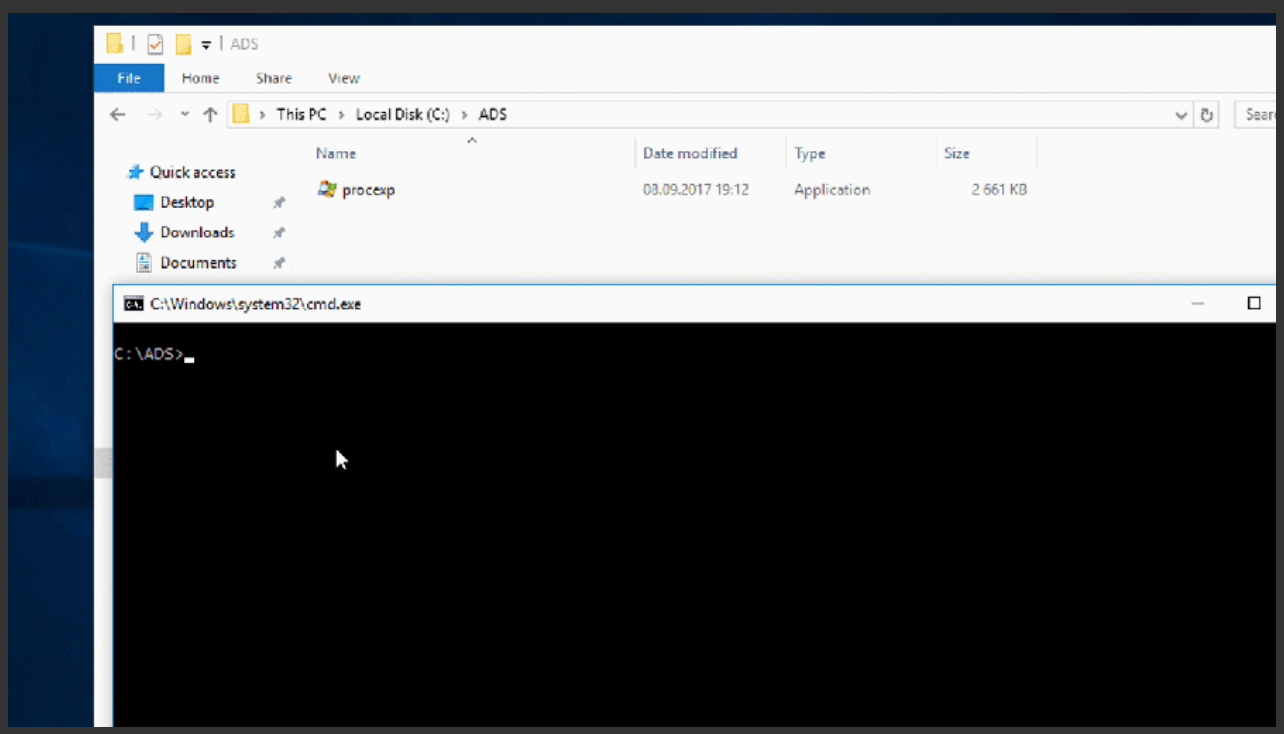
Also in my research I found that Findstr can also be used to inject a payload into another file as an ADS stream. Findstr.exe is basically a command you use to find strings within files. More about the binary here: https://ss64.com/nt/findstr.html

The cool thing I figured out was that you can search for a string that does not exist in a file and pipe that into a new file. And the cool thing is that it does allow it to be piped into a ADS stream of a file. It looks like this:

```
echo "empty file" > c:\ADS\file.txt
findstr /V /L W3AllLov3DonaldTrump c:\ADS\procexp.exe > c:\ADS\fil
```

```
wmic process call create '"c:\ADS\file.txt:procexp.exe"'
```

The /V in the findstr command makes sure that everything that does not match the string I am searching for is showed. 🙄

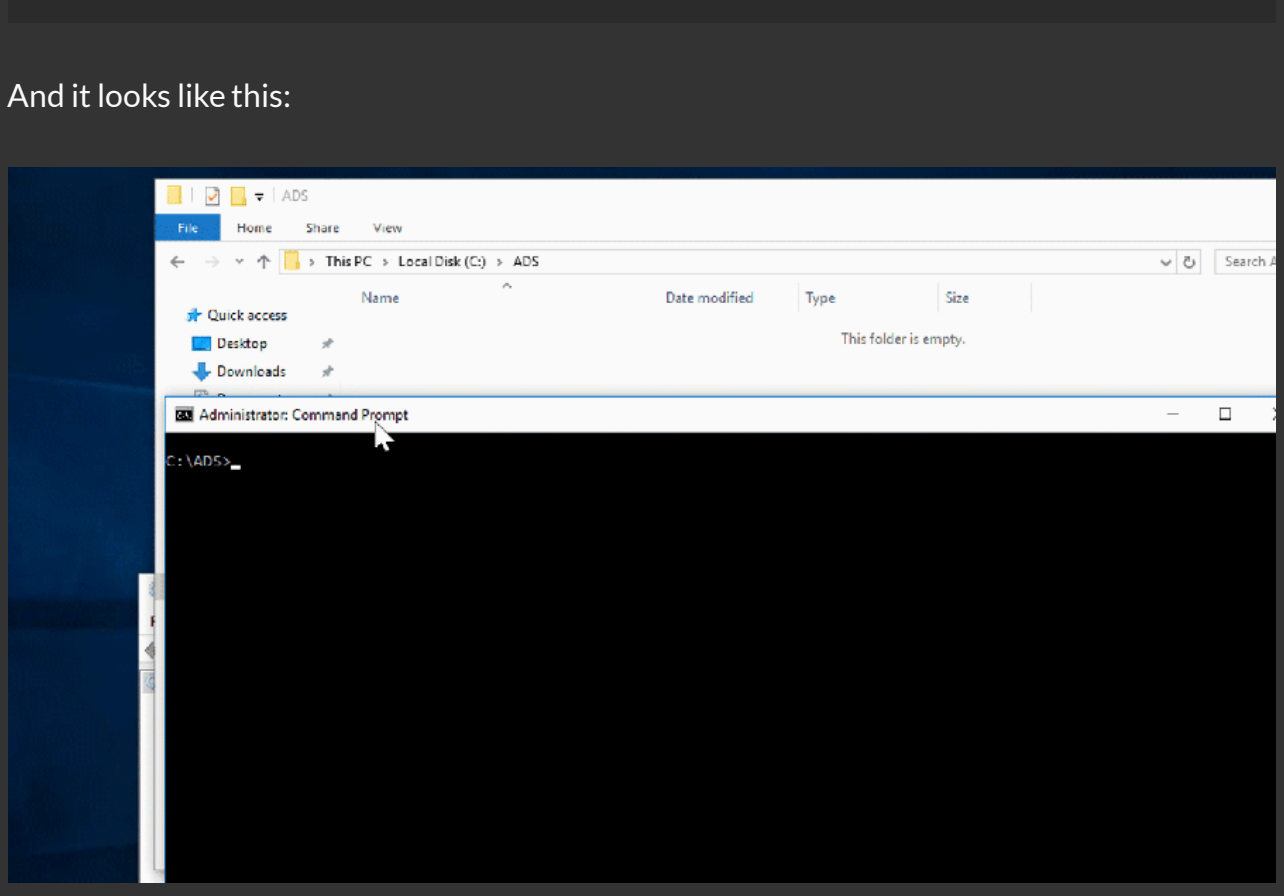


Executing ADS binary

I found another way to execute a binary from a alternate data stream when I was digging into this. It is possible to create a service in Windows (this requires local admin rights) that executes content from an Alternate Data Stream. I use the SC command to execute the necessary commands to create the service as want using these commands:

```
echo "empty file" > c:\ADS\file.txt
type c:\windows\system32\cmd.exe > c:\ADS\file.txt:cmd.exe
sc create evilservice binPath= "\"c:\ADS\file.txt:cmd.exe\" /c echo works > \"c:\ADS\works.txt
sc start evilservice
```

And it looks like this:



That's all for this time. I have also updated my ADS gist here for other methods: https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f

Hope you liked the post and as always I appreciate feedback. 🙄

RELATED

Putting data in Alternate data streams and how to execute it
14 Jan 2018
In "Security"

Persistence using GlobalFlags in Image File Execution Options – Hidden from Autoruns.exe
10 Apr 2018
In "Security"

A small discovery about AppLocker
29 May 2019
In "Security"

PREVIOUS POST
Persistence using GlobalFlags in Image File Execution Options – Hidden from Autoruns.exe

NEXT POST
GPscript.exe – another LOLBin to the list

16 THOUGHTS ON "PUTTING DATA IN ALTERNATE DATA STREAMS AND HOW TO EXECUTE IT – PART 2"

Pingback: Putting data in Alternate data streams and how to execute it – Oddvar Moe's Blog

Pingback: ADS数据流 第二篇 – 即刻安全

Pingback: Putting data in Alternate data streams and how to execute it – part 2 – Information Security Outsider

Pingback: Execute from Alternate Streams | websec blog

marc ochsenmeier (@ochsenmeier) says: 6 Oct 2018 at 12:59 pm

What about adding a section about the Win32 APIs that can be used to start executable located in ADS?
e.g. WinExec, CreateProcess, ShellExecute, ….

★ Like
Reply

★ **Oddvar Moe [MVP]** says: 7 Oct 2018 at 10:24 pm

That could be smart. You should start a post about it since you have some mapped out already

★ Like
Reply

Mike G. says: 16 Jan 2019 at 6:51 am

I may be way off track here but a few years back I was trying to find a way to embed the URL for a downloaded file into the name of the file when it was downloaded. This so that if I had a folder full of various documents and utilities accumulated over time, I could always have a way of finding the location on the web where I originally found the file I wanted to work with.
At the time, in theory, it sounded like it was something that could be done. But over time, I was never able to locate any code that could be employed to load the URL into an alternate stream of the file. Much the same as 'Exif' data is stored for a photo to show where it was taken and other details about it.
You seem to be extremely well versed on the subject. When I ran across your blog I remembered my old project and wondered if anything had changed that might make this more possible. Or maybe there is a better way that isn't so complex? The thought was to not have to do any more than drag and drop or download any file and have the URL it came from being added to one of the alt data streams attached to the file-name. Using the same technique in reverse, maybe via a ctrl+right click options could open the URL that the original file came from. Or am I stretching it too far?

★ Like
Reply

★ **Oddvar Moe [MVP]** says: 16 Jan 2019 at 9:49 am

Hi. Not sure but you can checkout page 15 in this pdf https://winitor.com/pdf/NtfsAlternateDataStreams.pdf. It seems someone is doing something similar already. 😳

★ Like
Reply

Pingback: A small discovery about AppLocker – Oddvar Moe's Blog

Pingback: Vulners weekly digest #2 – Vulners Blog

Pingback: RED TEAMING_Final Att&ck – B4cKD00₹

Ron says: 17 Mar 2021 at 4:46 pm

I have an ADS in a file:
17/03/2021 17:27 100 test2.txt
10 test2.txt:1:$DATA
1 File(s) 100 bytes
0 Dir(s) some bytes free
which I got by type somefile > test2.txt:1 resulting in 10 byte ADS correctly.
But when I DonaldTrump it from ADS to separate file, I get extra 2 bytes:
findstr /V /L W3AllLov3DonaldTrump test.exe

How do I avoid this (and get a 10 byte file like the original instead of a 12 byte file)?

★ Like
Reply

Ron says: 17 Mar 2021 at 4:48 pm

findstr /V /L W3AllLov3DonaldTrump test.exe

★ Like

Reply

Ron says: 17 Mar 2021 at 4:48 pm

"findstr /V /L W3AllLov3DonaldTrump test.exe"

★ Like

Reply

Ron says: 17 Mar 2021 at 4:49 pm

findstr /V /L W3AllLov3DonaldTrump test.exe

★ Like

Reply

Ron says: 17 Mar 2021 at 4:50 pm

This site won't let me post the correct code:
findstr /V /L W3AllLov3DonaldTrump left arrow test2.txt:1 right arrow test.exe

★ Like

Reply

LEAVE A COMMENT

This site uses Akismet to reduce spam. Learn how your comment data is processed.

Search … SEARCH