

Forum:[Hack Forums](#)

Thread: [BINDING ON TXT FILES](#)

zodi121 - February 17, 2019, 2:47 pm

is it possible to bind my exe file on txt files and pdf please ?

Exodus - February 17, 2019, 2:48 pm

(Feb 17, 2019 03:47 PM)zodi121 Wrote: [\[CITE\]](#) is it possible to bind my exe file on txt files and pdf please ?

PDF's: Yes

TXT's: No.

zodi121 - February 17, 2019, 2:50 pm

(Feb 17, 2019 03:48 PM)Exodus Wrote: [\[CITE\]](#) PDF's: Yes

TXT's: No.

how on pdf's please

martianhax - February 17, 2019, 2:52 pm

(Feb 17, 2019 03:50 PM)zodi121 Wrote: [\[CITE\]](#) how on pdf's please yes on both.

zodi121 - February 17, 2019, 2:53 pm

(Feb 17, 2019 03:52 PM)martianhax Wrote: [\[CITE\]](#) yes on both.

any help please on how ?

Exodus - February 17, 2019, 2:56 pm

(Feb 17, 2019 03:50 PM)zodi121 Wrote: [\[CITE\]](#) how on pdf's please

With a pdf exploit.

CyberStrike - February 17, 2019, 2:59 pm

(Feb 17, 2019 03:47 PM)zodi121 Wrote: [\[CITE\]](#) is it possible to bind my exe file on txt files and pdf please ?

I wouldn't use it as the premier method of landing on a target.. this said txt's you can use alternate data streams, generally this is more of a post exploitation move. eg.

type backdoor.exe C:\path\to\file.txt:backdoor.exe

Once again it's more post exploitation.

See PDF's often you are going to be looking at an exploit, note that there multiple pdf viewers/readers out there. Nothing prevent's one from including a link in a PDF to have a user manually download a payload themselves.

aerohacker - February 17, 2019, 9:42 pm

(Feb 17, 2019 03:59 PM)SilentWatch Wrote: [\[CITE\]](#) I wouldn't use it as the premier method of landing on a target.. this said txt's you can use alternate data streams, generally this is more of a post exploitation move. eg.

type backdoor.exe C:\path\to\file.txt:backdoor.exe

Once again it's more post exploitation.

See PDF's often you are going to be looking at an exploit, note that there multiple pdf viewers/readers out there. Nothing prevent's one from including a link in a PDF to have a user manually download a payload themselves.

There's a lot of DOC, XLS, PPT and PDF Exploits, but there's JPEG, MP3 and AVI Exploits?

PerfectStorm - February 17, 2019, 9:46 pm

There is .doc .pdf .xls ect. ect. but not .txt no.

CyberStrike - February 17, 2019, 11:45 pm

(Feb 17, 2019 03:59 PM)SilentWatch Wrote: [\[CITE\]](#) I wouldn't use it as the premier method of landing on a target.. this said txt's you can use alternate data streams, generally this is more of a post exploitation move. eg.

type backdoor.exe C:\path\to\file.txt:backdoor.exe

Once again it's more post exploitation.

See PDF's often you are going to be looking at an exploit, note that there multiple pdf viewers/readers out there. Nothing prevent's one from including a link in a PDF to have a user manually download a payload themselves.

(Feb 17, 2019 10:42 PM)aerohacker Wrote: [\[CITE\]](#) There's a lot of DOC, XLS, PPT and PDF Exploits, but there's JPEG, MP3 and AVI Exploits?

I was not talking an exploit I more am thinking of a post exploitation where a txt file is used. It's pretty old well over 4 years old

http://techgenix.com/Alternate_Data_Streams/

<https://enigma0x3.net/2015/03/05/using-alternate-data-streams-to-persist-on-a-compromised-machine/>

It isn't an "exploit" it's just how NTFS works, I do believe as of a year and half or so ago this evaded a FEW AV's not sure on how it does now although let us remember that being an administrator of the machine you land upon is important so adding it to the exclusions is an option.

As for MP3 I remember a file exploit where it would basically overflow a buffer and give you a shell. Remember that it's often geared towards a specific player. JPEG I know was made into a polyglot payload against a web app much like we see in bmp/png. Some files have VERY loose tolerances just look at jar's and zip files very much the same header. There are a few POC's out there for polyglot file types, of course decrypting the file on target and execution will be a big hurdle.

I tend to like using this example to illustrate the loose tolerances, since it's common place to rename a jar as a zip and start taking it apart.

Quote:Zip:

```
00000000 50 4b 03 04 14 03 01 00 08 00 04 b2 38 4e 9f 39 |PK.....8N.9|
00000010 8f 08 ca 6d 02 00 00 2e 03 00 0f 00 00 00 57 68 |...m.....Wh|
00000020 69 74 65 6c 69 73 74 65 72 2e 62 69 6e 71 b2 d6 |itelister.binq..|
00000030 b0 7a 25 82 6d 93 e2 47 49 f7 cf 03 dc d9 51 ba |.z%.m..GI.....Q.|
00000040 99 38 04 9d 15 fa d3 04 44 11 46 df 1d a3 ed 72 |.8.....D.F....r|
00000050 02 51 19 ad 0f c9 bd f5 4c 03 e4 b1 f3 fe 1b ad |.Q.....L.....|
```

```
00000060 44 73 ce ec 18 2a c1 a8 83 ee e1 2a 62 43 26 de |Ds...*.....*bC&|
00000070 5b 9f a0 ee 79 c4 d3 b0 76 48 8a c0 b8 5f c7 e5 | [...y...vH..._|
00000080 1a bd 5c 04 08 e1 c4 ad 41 04 de 66 29 d8 92 bb |..\.....A..f)...|
00000090 b6 e9 4b dd c1 68 41 f6 7d f7 e7 f3 ec 93 6e f2 |..K..hA.}.....n.|
```

Quote:Jar:

```
00000000 50 4b 03 04 0a 00 00 08 08 00 f1 39 fe 4c 00 00 |PK.....9.L..|
00000010 00 00 02 00 00 00 00 00 00 00 09 00 00 00 4d 45 |.....ME|
00000020 54 41 2d 49 4e 46 2f 03 00 50 4b 03 04 0a 00 00 |TA-INF/..PK.....|
00000030 08 08 00 f1 39 fe 4c 02 ea 4f 22 5a 01 00 00 4d |....9.L..O"Z...M|
00000040 02 00 00 14 00 00 00 4d 45 54 41 2d 49 4e 46 2f |.....META-INF/|
00000050 4d 41 4e 49 46 45 53 54 2e 4d 46 6d 91 cd 8a dc |MANIFEST.MFm....|
00000060 40 0c 84 ef 06 bf 83 5f c0 b3 96 fa 4f ed 63 72 |@....._.....O.cr|
00000070 da c3 84 80 21 e4 aa 56 ab 1d c3 8e 67 b0 bd e4 |....!..V....g...|
00000080 f5 d3 24 de 85 b0 7b d0 a5 ea ab 92 9a be f2 ba |..$...{.....|
00000090 14 dd 8f fe 87 6e fb 72 5f c7 0e 2e 43 db 3c df |.....n.r_...C.<.|
```

Hypnotist - February 18, 2019, 1:05 am

Check out .lnk files, you can change the icon and make it download+execute your file. Search mLNK on hackforums they sell a FUD builder.

macpromo - February 19, 2019, 8:17 am

alternate data streams on NTFS systems. for PDF use exploits