

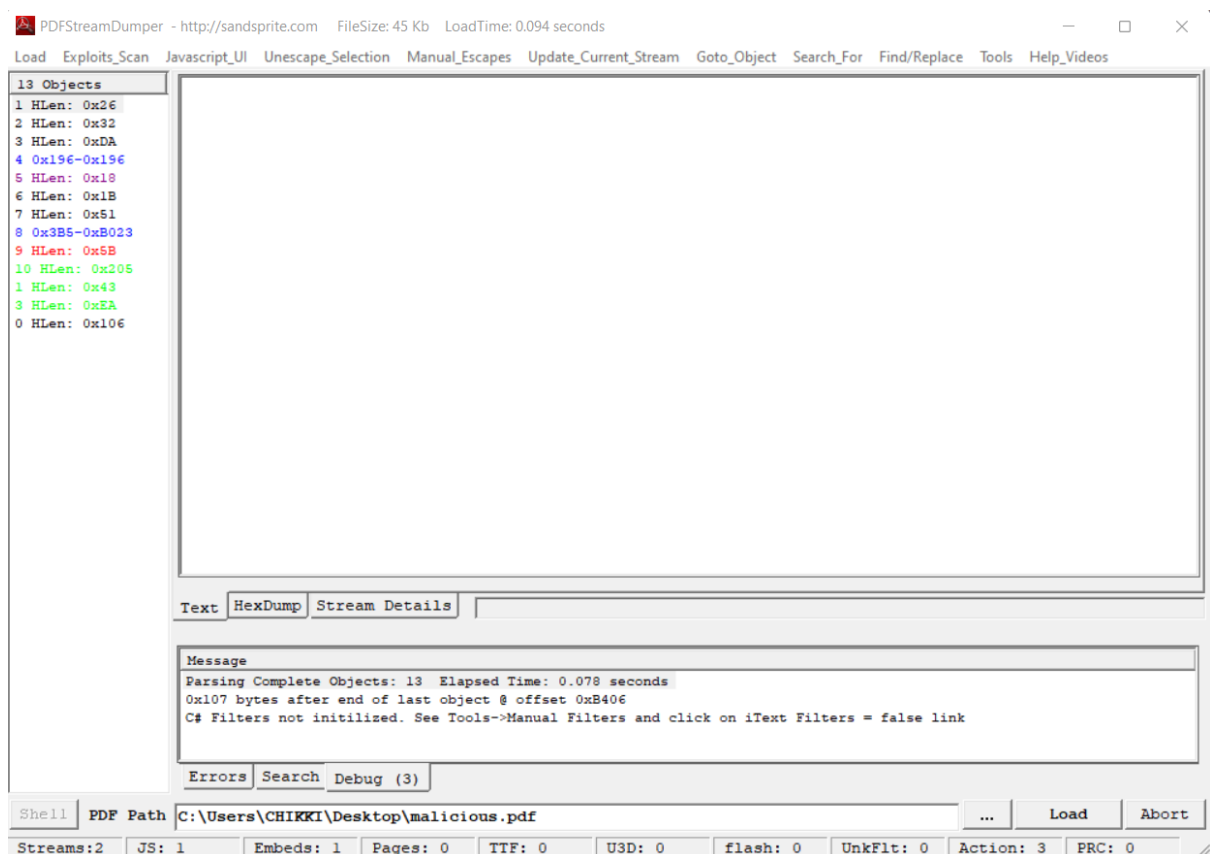
Malicious PDF File Analysis -

No. 16

Stage 2: Your job is to investigate the content of a given malicious pdf file. Using the PDF analysing tools offered by the REMnux tool, spider monkey, sctest, or PDF Stream Dumper, address the following questions/activities.

1-Report the number of objects in the file.

There are 13 objects in the given file.



2-Determine whether the file is compressed or not.

Yes, the file is compressed.

The screenshot shows the PDFStreamDumper application interface. The left pane lists 13 objects, with object 8 selected. The main pane displays the details for Object Index 8:

```
Object Index: 8
Object Start Offset: 0x322 (802)
Object End Offset: 0xB034 (45108)
Stream Start Offset: 0x3B5 (949)
Stream End Offset: 0xB023 (45091)
Compressed Size: 0xAC6E (44142)
Compressed CRC: 0xAACBD82F
DecompFilters: FlateDecode
Unsupported Filters?: False
DeCompressed Size: 0x1204A (73802)
DeCompressed CRC: 0x31FED0FD
Expansion Ratio: 1.67x (29660 bytes)
Detected Type:.unk
HeaderCRC: 86D8A321
Header:

<<
  /Subtype/application/pdf/Length 44145/Filter/FlateDecode/DL 73802/Params
  <<
    /Size 73802/Checksum<B7FF74AD2ED1BB98074C1652D8C25F3F
  >>
  >>
```

Below the object details, the 'Message' pane shows parsing information:

```
Parsing Complete Objects: 13 Elapsed Time: 0.094 seconds
0x107 bytes after end of last object @ offset 0xB406
C# Filters not initialized. See Tools->Manual Filters and click on iText Filters = false link
```

The bottom status bar shows file statistics: Streams: 2, JS: 1, Embeds: 1, Pages: 0, TTF: 0, U3D: 0, flash: 0, UnkFlt: 0, Action: 3, PRC: 0.

3. Determine whether the file is obfuscated or not.

Yes, the file is obfuscated.

The screenshot shows the PDFStreamDumper application interface. The left pane lists 13 objects, with object 9 selected. The main pane displays the details for Object Index 9:

```
Object Index: 9
Object Start Offset: 0xB03A (45114)
Object End Offset: 0xB09F (45215)
Detected Type:.unk
HeaderCRC: A7BA13F5
Header:

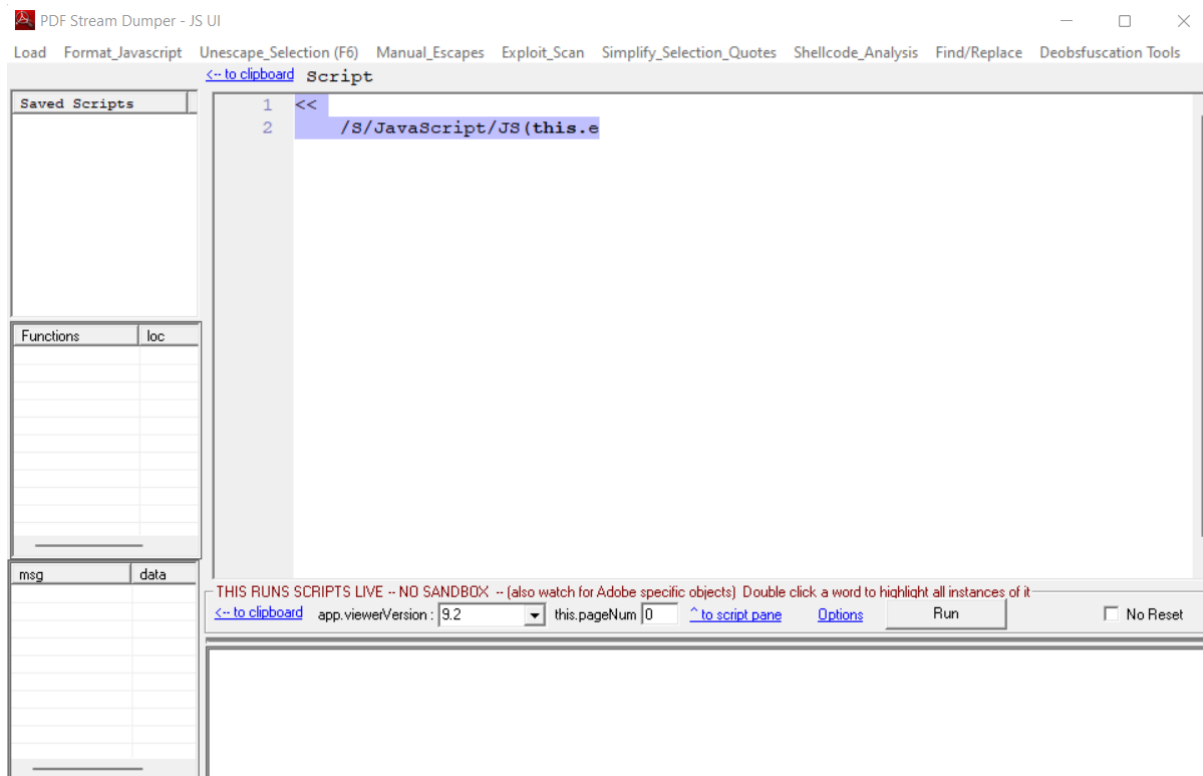
<<
  /S/JavaScript/JS(this.exportDataObject({cName: "template", nLaunch: 0
  >>
```

A Notepad window is open over the object details, displaying the following text:

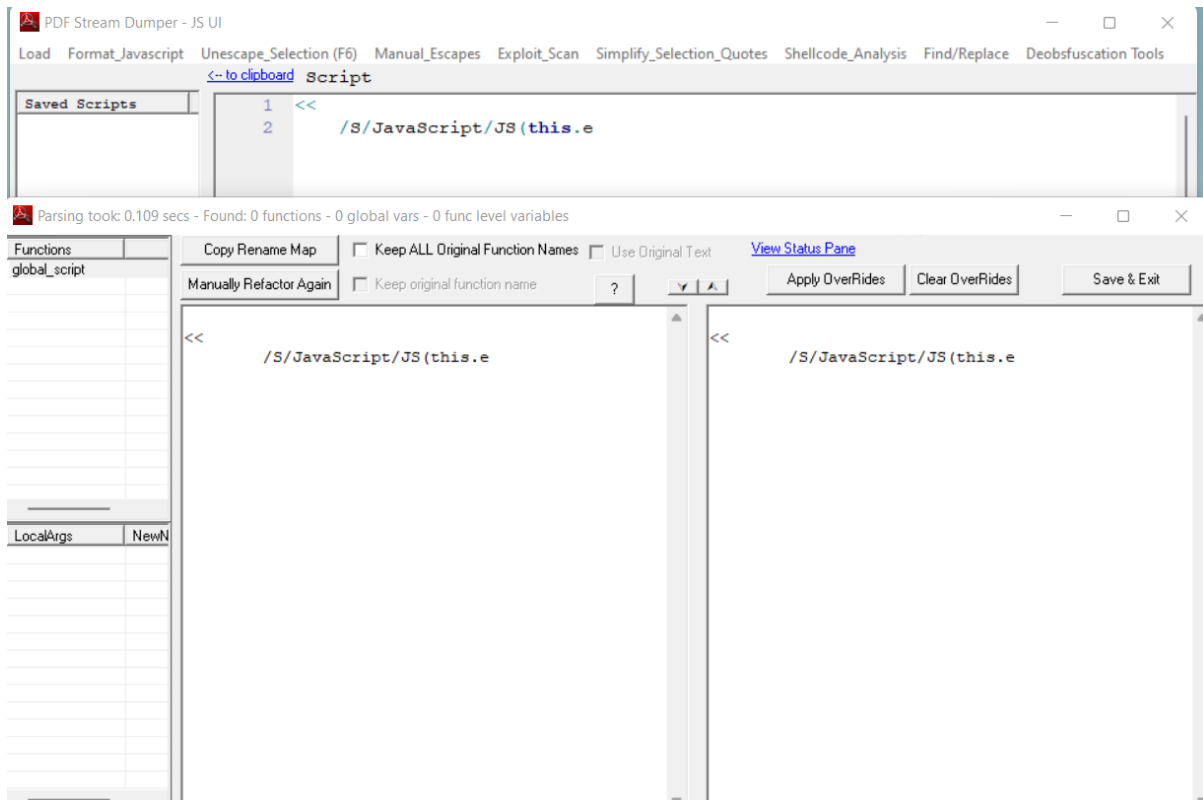
```
1766661929 - Notepad
File Edit View
Exploit Header contains a Launch Action - possible CVE-2010-1240 Date:6.29.10 v9.3.2 - */Launch*/Acti
Note other exploits may be hidden with javascript obfuscation
It is also possible these functions are being used in a non-exploit way.
Ln 3, Col 63 100% Windows (CRLF) UTF-8
```

The bottom status bar shows file statistics: Streams: 2, JS: 1, Embeds: 1, Pages: 0, TTF: 0, U3D: 0, flash: 0, UnkFlt: 0, Action: 3, PRC: 0.

4. Find and Extract JavaScript.



5. De-obfuscate JavaScript.



6. Extract the shell code.

No shell code found.

7. Create a shell code executable

As there is no shell code found, unable to create shell code executable.

8. Analyse shell code and determine what it does or even execute it using sctest or spider monkey

Unable to analyse as there is no shell code.

9. What is the secret code?

No secret code found.