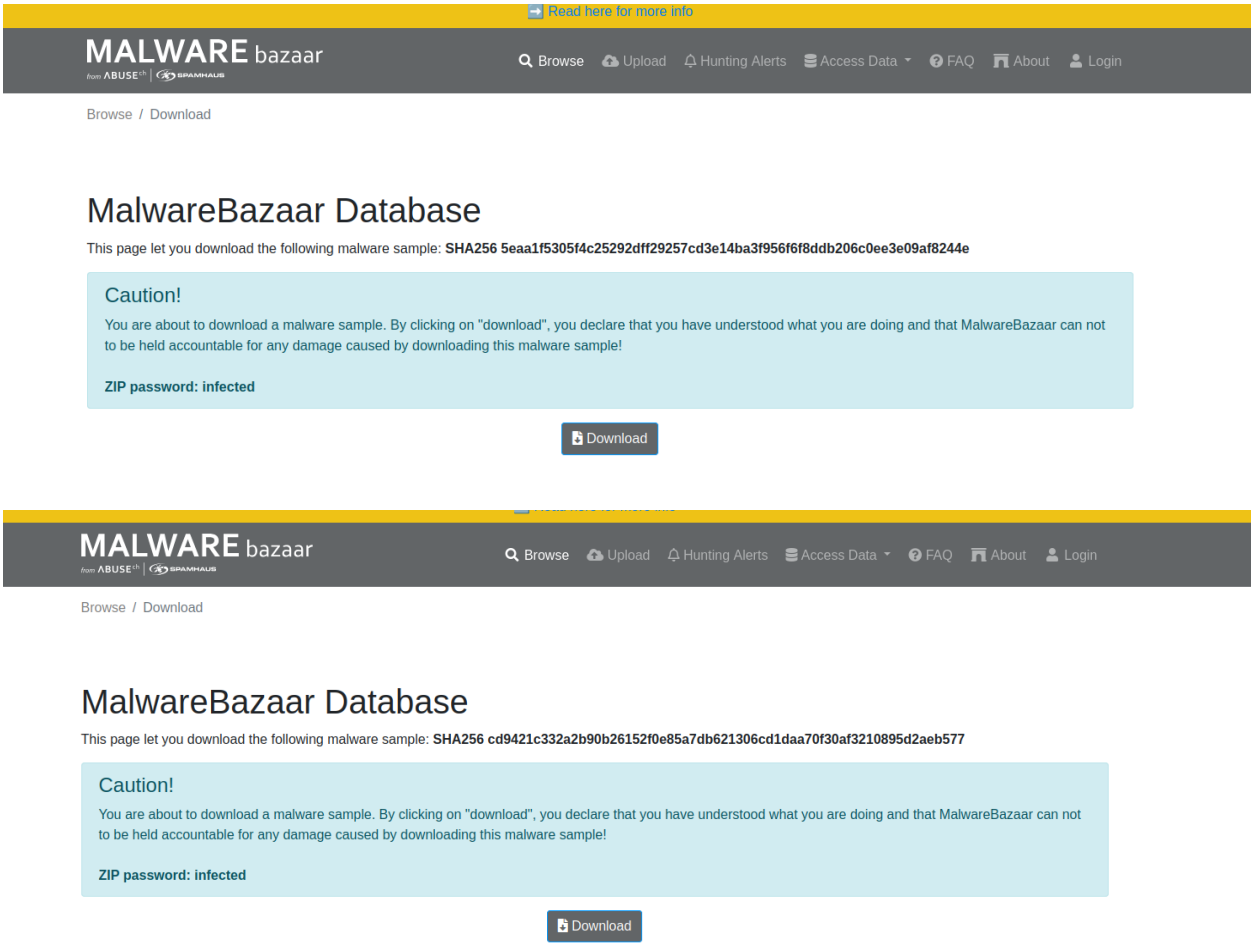
Step 0 — Download The Files



1. Create a folder for PDF samples:

mkdir ~/malware_pdfs

cd ~/malware_pdfs

```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~/DidierStevensSuite$ mkdir ~/malware_pdfs
cd ~/malware_pdfs
```

2. Move or copy downloaded ZIP files into this folder.

3. Use 7-Zip to extract PDFs:

7z x cd9421c332a2b90b26152f0e85a7db621306cd1daa70f30af3210895d2aeb577.zip

7z x 5eaa1f5305f4c25292dff29257cd3e14ba3f956f6f8ddb206c0ee3e09af8244e.zip

```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~/malware_pdfs$ 7z x cd9421c332a2b90b26152f0e85a7db621306cd1daa70f30af3210895d2aeb577.zip
7z x 5eaa1f5305f4c25292dff29257cd3e14ba3f956f6f8ddb206c0ee3e09af8244e.zip

7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
 64-bit locale=en_US.UTF-8 Threads:128 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 499220 bytes (488 KiB)

Extracting archive: cd9421c332a2b90b26152f0e85a7db621306cd1daa70f30af3210895d2aeb577.zip
--
Path = cd9421c332a2b90b26152f0e85a7db621306cd1daa70f30af3210895d2aeb577.zip
Type = zip
Physical Size = 499220


Enter password (will not be echoed):
Everything is Ok

Size:       509814
Compressed: 499220

7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
 64-bit locale=en_US.UTF-8 Threads:128 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 25021 bytes (25 KiB)

Extracting archive: 5eaa1f5305f4c25292dff29257cd3e14ba3f956f6f8ddb206c0ee3e09af8244e.zip
--
Path = 5eaa1f5305f4c25292dff29257cd3e14ba3f956f6f8ddb206c0ee3e09af8244e.zip
Type = zip
Physical Size = 25021


Enter password (will not be echoed):
Everything is Ok
```

Step 1 — Quick Scan with PDFiD

Scan PDFs for suspicious elements:

python3 ~/DidierStevensSuite/pdfid.py -e

cd9421c332a2b90b26152f0e85a7db621306cd1daa70f30af3210895d2aeb577.pdf

```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~/malware_pdfs$ python3 ~/DidierStevensSuite/pdfid.py -e cd9421c332
a2b90b26152f0e85a7db621306cd1daa70f30af3210895d2aeb577.pdf
python3 ~/DidierStevensSuite/pdfid.py -e 5eaa1f5305f4c25292dff29257cd3e14ba3f956f6f8ddb206c0ee3e09af8244e.pdf
PDFiD 0.2.10 cd9421c332a2b90b26152f0e85a7db621306cd1daa70f30af3210895d2aeb577.pdf
 PDF Header: %PDF-1.4
 obj                   56
 endobj                56
 stream                21
 endstream             21
 xref                   2
 trailer                2
 startxref              2
 /Page                  7
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            2
 /AA                    0
 /OpenAction            0
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          0
 /XFA                   0
 /URI                   0
 /Colors > 2^24         0
 %%EOF                  2
 After last %%EOF       0
 D:20210805114807+09'00  /CreationDate
 D:20210805114809+09'00  /CreationDate
 D:20210805114809+09'00  /ModDate
 Total entropy:           7.980886 (    509814 bytes)
 Entropy inside streams:  7.983494 (    499762 bytes)
 Entropy outside streams: 5.225614 (     10052 bytes)
```

```
PDFiD 0.2.10 5eaa1f5305f4c25292dff29257cd3e14ba3f956f6f8ddb206c0ee3e09af8244e.pdf
 PDF Header: %PDF-1.6
 obj                    33
 endobj                 33
 stream                 30
 endstream              30
 xref                    0
 trailer                 0
 startxref               2
 /Page                   1
 /Encrypt                0
 /ObjStm                 4
 /JS                     0
 /JavaScript             0
 /AA                     0
 /OpenAction             0
 /AcroForm               0
 /JBIG2Decode            0
 /RichMedia              0
 /Launch                 0
 /EmbeddedFile           0
 /XFA                    0
 /URI                    0
 /Colors > 2^24          0
 %%EOF                   2
 After last %%EOF        0
 Total entropy:           7.594188 (     31276 bytes)
 Entropy inside streams:  7.699941 (     26320 bytes)
 Entropy outside streams: 5.340535 (      4956 bytes)
```

- /JS, /JavaScript → embedded scripts
- /OpenAction → actions on open
- /AA → automatic actions
- /Launch → launches external programs
- /EmbeddedFile → embedded files

Step 2 — Detailed Analysis with pdf-parser

1. Get stats for each PDF:

python2 ~/DidierStevensSuite/pdf-parser.py cd9421c332a2b90b26152f0e85a7db621306cd1daa70f30af3210895d2aeb577.pdf -a

python2 ~/DidierStevensSuite/pdf-parser.py 5eaa1f5305f4c25292dff29257cd3e14ba3f956f6f8ddb206c0ee3e09af8244e.pdf -a

```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~/malware_pdfs$ python2 ~/DidierStevensSuite/pdf-parser.py cd9421c332a2b90b26152f0e85a7db621306cd1daa70f30af3210895d2
aeb577.pdf -a
python2 ~/DidierStevensSuite/pdf-parser.py 5eaa1f5305f4c25292dff29257cd3e14ba3f956f6f8ddb206c0ee3e09af8244e.pdf -a
Comment: 4
XREF: 2
Trailer: 2
StartXref: 2
Indirect object: 56
Indirect objects with a stream: 30, 25, 40, 32, 42, 34, 44, 36, 46, 38, 4, 6, 8, 10, 12, 14, 18, 16, 47, 52, 54
  24: 30, 40, 32, 42, 34, 44, 36, 46, 38, 4, 6, 8, 10, 12, 14, 18, 16, 48, 49, 50, 51, 52, 54, 55
 /Catalog 2: 19, 19
 /ExtGState 4: 21, 22, 23, 24
 /Filespec 1: 53
 /Font 10: 26, 27, 28, 29, 31, 33, 35, 37, 3, 15
 /FontDescriptor 5: 39, 41, 43, 45, 17
 /Metadata 1: 47
 /Page 7: 20, 2, 5, 7, 9, 11, 13
 /Pages 1: 1
 /XObject 1: 25
Search keywords:
 /JS 1: 51
 /JavaScript 2: 48, 51
Comment: 4
XREF: 0
Trailer: 0
StartXref: 2
Indirect object: 33
Indirect objects with a stream: 37, 63, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 1, 2, 3, 4, 5
  13: 11, 63, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 35
 /Catalog 1: 12
 /Metadata 1: 2
 /ObjStm 4: 22, 1, 3, 4
 /Page 1: 13
 /XObject 11: 14, 15, 16, 17, 18, 19, 20, 21, 33, 34, 36
 /XRef 2: 37, 5
Unreferenced indirect objects: 1 0 R, 3 0 R, 4 0 R, 5 0 R, 11 0 R, 13 0 R, 14 0 R, 17 0 R, 20 0 R, 21 0 R, 22 0 R, 24 0 R, 25 0 R, 26 0 R, 27 0 R, 28 0 R, 29 0 R,
30 0 R, 31 0 R, 32 0 R, 35 0 R, 37 0 R, 63 0 R
Unreferenced indirect objects without /ObjStm objects: 5 0 R, 11 0 R, 13 0 R, 14 0 R, 17 0 R, 20 0 R, 21 0 R, 24 0 R, 25 0 R, 26 0 R, 27 0 R, 28 0 R, 29 0 R, 30 0
```

2. Search for JavaScript or OpenAction objects:

python2 ~/DidierStevensSuite/pdf-parser.py cd9421c332a2b90b26152f0e85a7db621306cd1daa70f30af3210895d2aeb577.pdf --search /JavaScript

python2 ~/DidierStevensSuite/pdf-parser.py cd9421c332a2b90b26152f0e85a7db621306cd1daa70f30af3210895d2aeb577.pdf --search /OpenAction

```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~/malware_pdfs$ python2 ~/DidierStevensSuite/pdf-parser.py cd9421c332a2b90b26152f0e85a7db621306cd1daa70f30af3210895d2
aeb577.pdf --search /JavaScript
python2 ~/DidierStevensSuite/pdf-parser.py cd9421c332a2b90b26152f0e85a7db621306cd1daa70f30af3210895d2aeb577.pdf --search /OpenAction
obj 48 0
 Type:
 Referencing: 49 0 R, 50 0 R

  <<
    /EmbeddedFiles 49 0 R
    /JavaScript 50 0 R
  >>


obj 51 0
 Type:
 Referencing: 52 0 R

  <<
    /JS 52 0 R
    /S /JavaScript
  >>
```

3. Note suspicious objects (e.g., 48, 50, 51, 52) for extraction.

Step 3 — Extract Suspicious Objects

Extract JavaScript

python2 ~/DidierStevensSuite/pdf-parser.py cd9421c332a2b90b26152f0e85a7db621306cd1daa70f30af3210895d2aeb577.pdf -o 50 --filter > object50.js

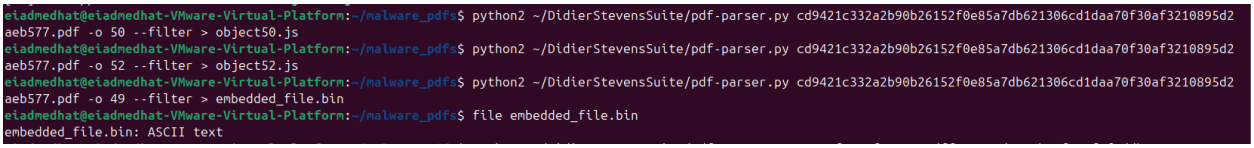
python2 ~/DidierStevensSuite/pdf-parser.py cd9421c332a2b90b26152f0e85a7db621306cd1daa70f30af3210895d2aeb577.pdf -o 52 --filter > object52.js

Extract embedded file

python2 ~/DidierStevensSuite/pdf-parser.py cd9421c332a2b90b26152f0e85a7db621306cd1daa70f30af3210895d2aeb577.pdf -o 49 --filter > embedded_file.bin

4. Check the file type:

file embedded_file.bin



Step 4 — Interactive Analysis with peepdf

- docInfo → Shows metadata and general info about the PDF.
- listObjects → Lists all objects in the PDF with their IDs.
- analyze <id> → Analyzes a specific object for suspicious content.
- javascript → Displays embedded JavaScript code within the PDF.
- disarm → Disables JavaScript and automatic actions for safe analysis

python2 ~/peepdf/peepdf.py
cd9421c332a2b90b26152f0e85a7db621306cd1daa70f30af3210895d2aeb577.pdf

```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~/malware_pdfs$ python2 ~/peepdf/peepdf.py cd9421c332a2b90b26152f0e85a7db621306cd1daa70f30af3210895d2aeb577.pdf
Warning: PyV8 is not installed!!
Warning: pylibemu is not installed!!
Warning: Python Imaging Library (PIL) is not installed!!

File: cd9421c332a2b90b26152f0e85a7db621306cd1daa70f30af3210895d2aeb577.pdf
MD5: 6d6399e5e98164e365029a9b141e1646
SHA1: 64f8b386000ed34f7b9f22a8144328d0e61ed31c
SHA256: cd9421c332a2b90b26152f0e85a7db621306cd1daa70f30af3210895d2aeb577
Size: 509814 bytes
Version: 1.4
Binary: True
Linearized: False
Encrypted: False
Updates: 1
Objects: 56
Streams: 21
URIs: 0
Comments: 0
Errors: 0

Version 0:
        Catalog: 19
        Info: No
        Objects (46): [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 3
8, 39, 40, 41, 42, 43, 44, 45, 46]
        Streams (18): [30, 25, 40, 32, 42, 34, 44, 36, 46, 38, 4, 6, 8, 10, 12, 14, 18, 16]
                Encoded (18): [30, 25, 40, 32, 42, 34, 44, 36, 46, 38, 4, 6, 8, 10, 12, 14, 18, 16]

Version 1:
        Catalog: 19
        Info: 55
        Objects (10): [19, 47, 48, 49, 50, 51, 52, 53, 54, 55]
        Streams (3): [47, 52, 54]
                Encoded (2): [52, 54]
        Objects with JS code (1): [52]
```

```
Suspicious elements:
        /Names (3): [19, 49, 50]
        /JavaScript (2): [48, 51]
        /JS (1): [51]
        /EmbeddedFiles: [48]
```

python2 ~/peepdf/peepdf.py
5eaa1f5305f4c25292dff29257cd3e14ba3f956f6f8ddb206c0ee3e09af8244e.pdf

```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~/malware_pdfs$ python2 ~/peepdf/peepdf.py 5eaa1f5305f4c25292dff29257cd3e14ba3f956f6f8ddb206c0ee3e09af8244e.pdf
Warning: PyV8 is not installed!!
Warning: pylibemu is not installed!!
Warning: Python Imaging Library (PIL) is not installed!!

File: 5eaa1f5305f4c25292dff29257cd3e14ba3f956f6f8ddb206c0ee3e09af8244e.pdf
MD5: 2c182c48da297dcee3c7cafab4e46161
SHA1: d031305516b4791ec52a2bd03450d185c16e8dd0
SHA256: 5eaa1f5305f4c25292dff29257cd3e14ba3f956f6f8ddb206c0ee3e09af8244e
Size: 31276 bytes
Version: 1.6
Binary: True
Linearized: True
Encrypted: False
Updates: 1
Objects: 63
Streams: 30
URIs: 1
Comments: 0
Errors: 0

Version 0:
        Catalog: 12
        Info: 10
        Objects (2): [11, 37]
        Streams (1): [37]
                Xref streams (1): [37]
                Encoded (1): [37]

Version 1:
        Catalog: 12
        Info: 10
        Objects (61): [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 38, 39, 4
0, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]
        Compressed objects (30): [38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 8, 6, 7, 9, 10]
        Streams (29): [63, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 1, 2, 3, 4, 5]
                Xref streams (1): [5]
                Object streams (4): [22, 1, 3, 4]
```

```
            Object streams (4): [22, 1, 3, 4]
            Encoded (22): [63, 16, 19, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 1, 3, 4, 5]
        Objects with URIs (1): [62]
```