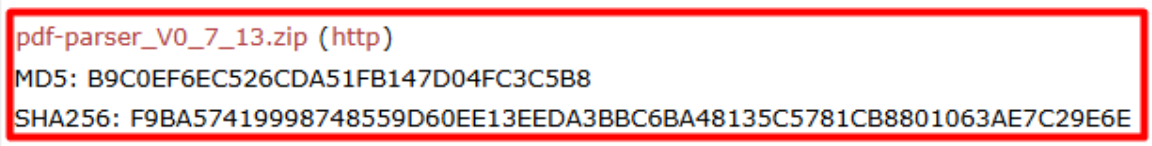
Suspicious pdf file analysis

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.

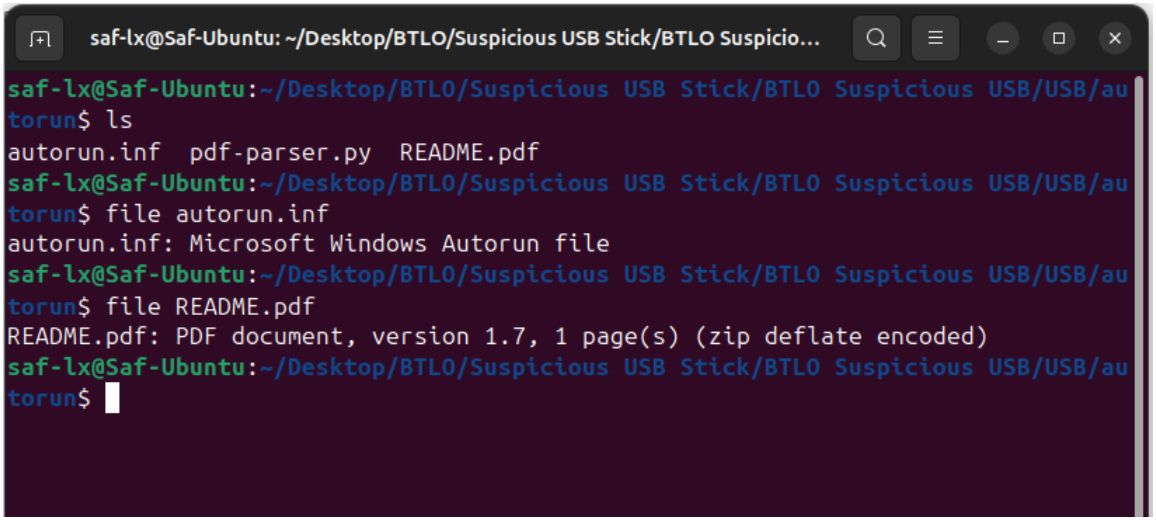
Files and pdf parser.

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

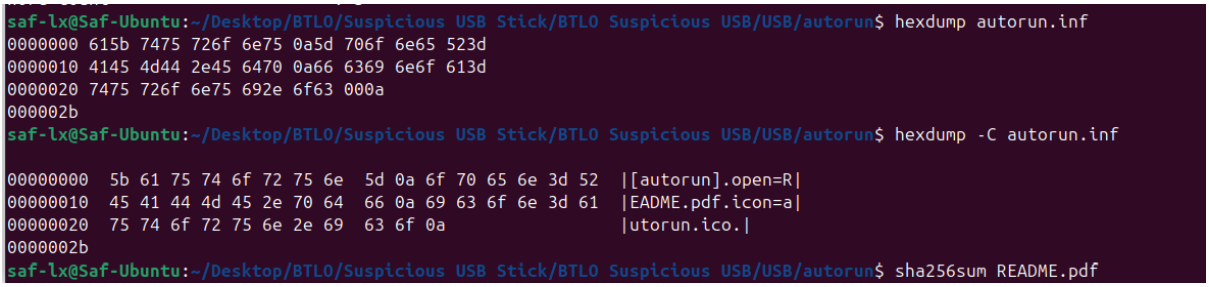


File description.

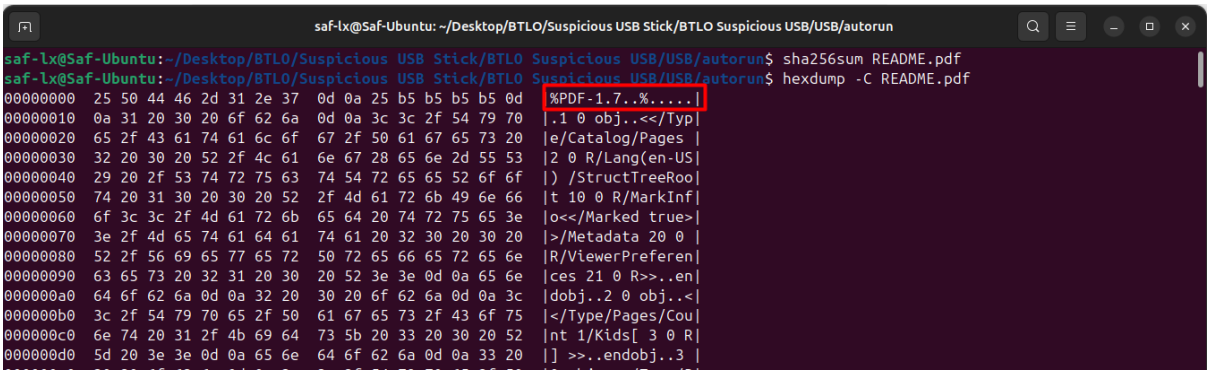
Suspicious pdf file analysis



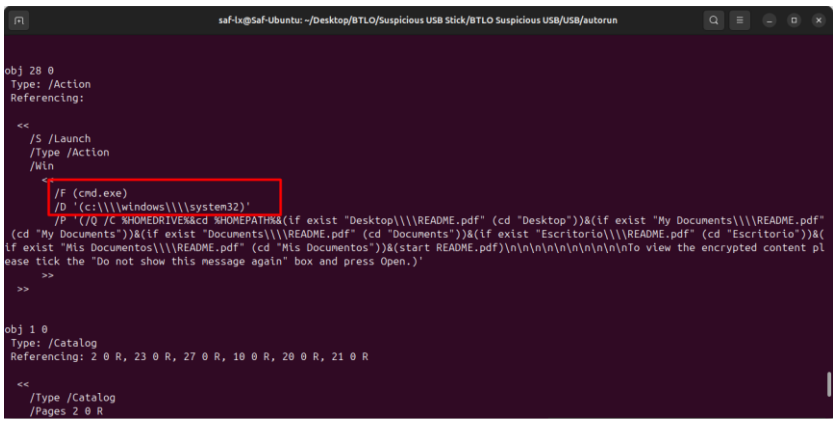
Hexdump of autorun.inf. It shows that it opens the README.pdf file.



Magic bits of pdf file

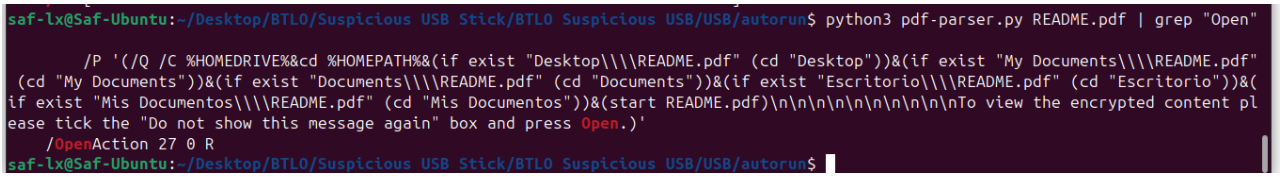


Executable file details.



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.



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

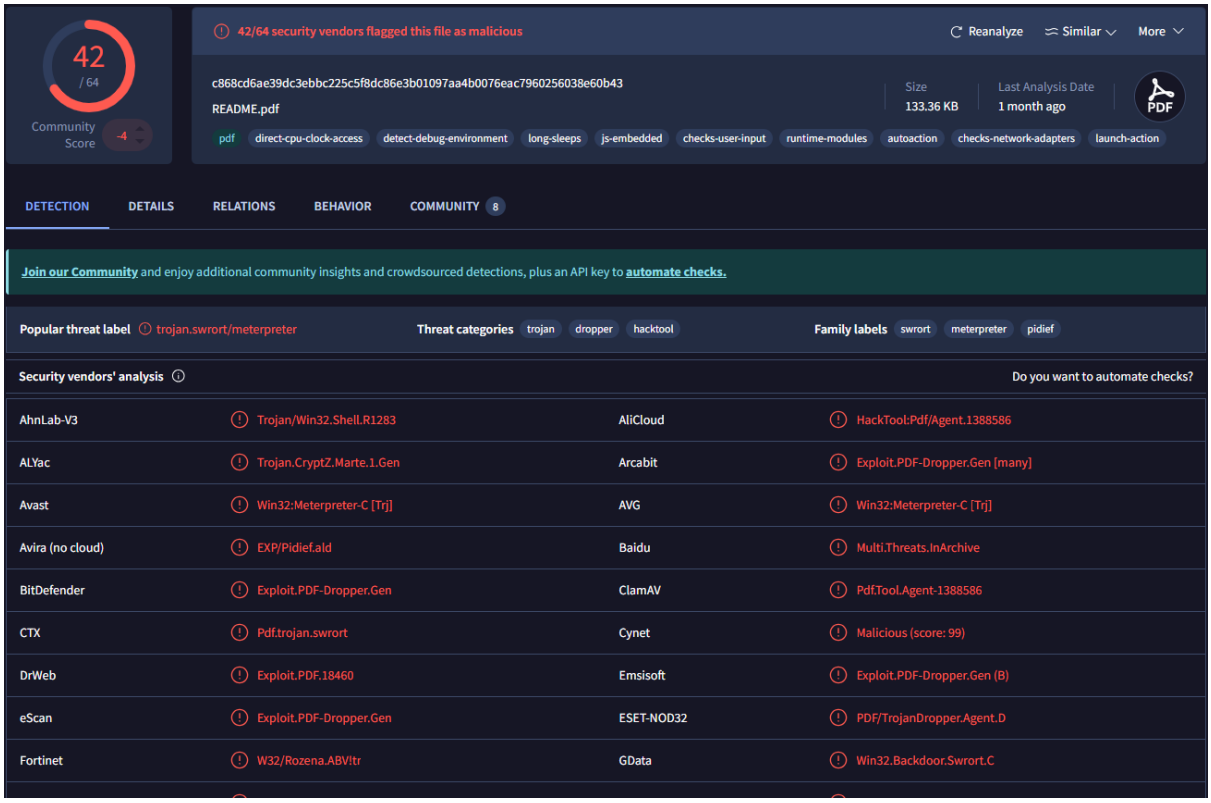
```
obj 27 0
 Type: /Action
 Referencing:

  <<
    /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



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.