Quick malicious PDF analysis: 1

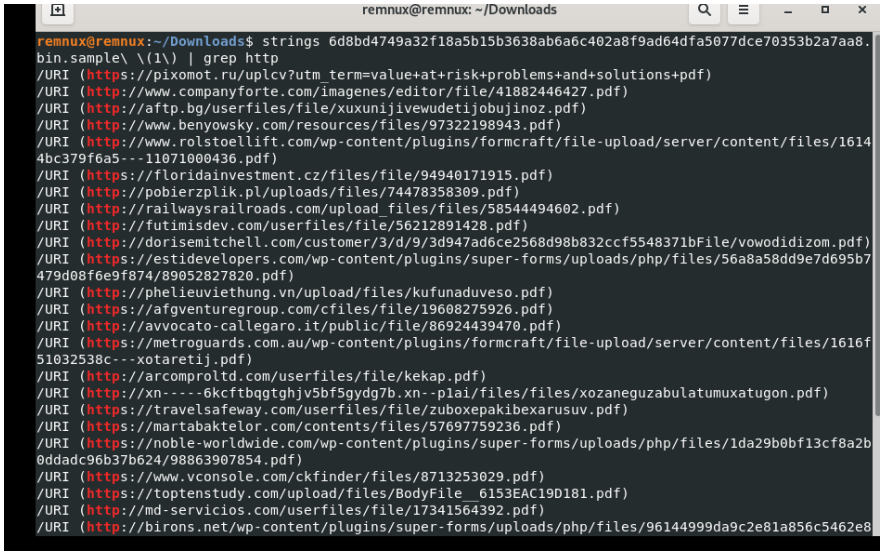
The following is an analysis of a labeled malicious PDF from Hybrid Analysis using REMnux in VirtualBox. It was labeled as a Trojan by Hybrid Analysis (Hybrid Analysis 2022).

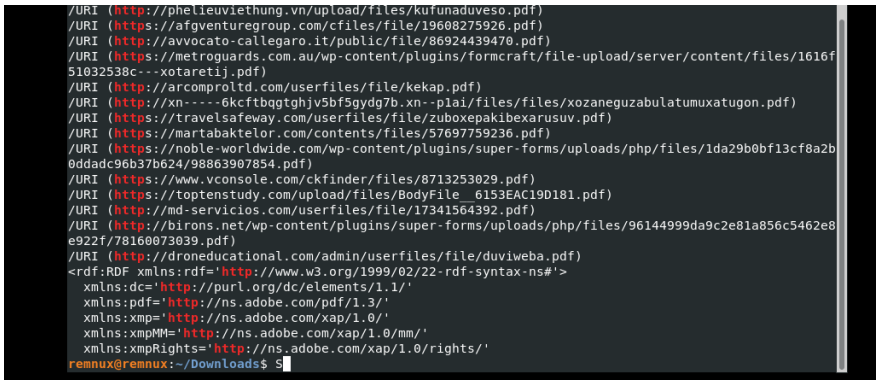
Upon downloading the file and unzipping it I dumped the strings of the file using :

```
strings | less
```

There was too much information to make sense of it, so I tried searching specifically for any http links using:

```
Strings | grep http
```





There are a large number of links, which is very suspicious.

Using pdfid and peepdf I had a more indepth look at the PDF. The title of the PDF is “Value at risk problems and solutions pdf”; a vague yet familiar enough name for someone in a corporate

environment to open to have a look. Unfortunately I didn't find any indication of Javascript or encryptions in the file that is generally a giveaway for a malicious file.

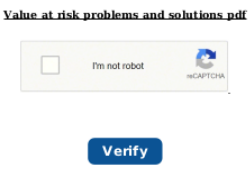
Obtained from peepdf:

```
File: 6d8bd4749a32f18a5b15b3638ab6a6c402a8f9ad64dfa5077dce70353b2a7aa8.bin.sample (1)
MD5: 1cded74d861bb3830ba835ec7a463021
SHA1: 661a8f9e8c6c934dfe83ddd232f7669c6bd487b3
SHA256: 6d8bd4749a32f18a5b15b3638ab6a6c402a8f9ad64dfa5077dce70353b2a7aa8
```

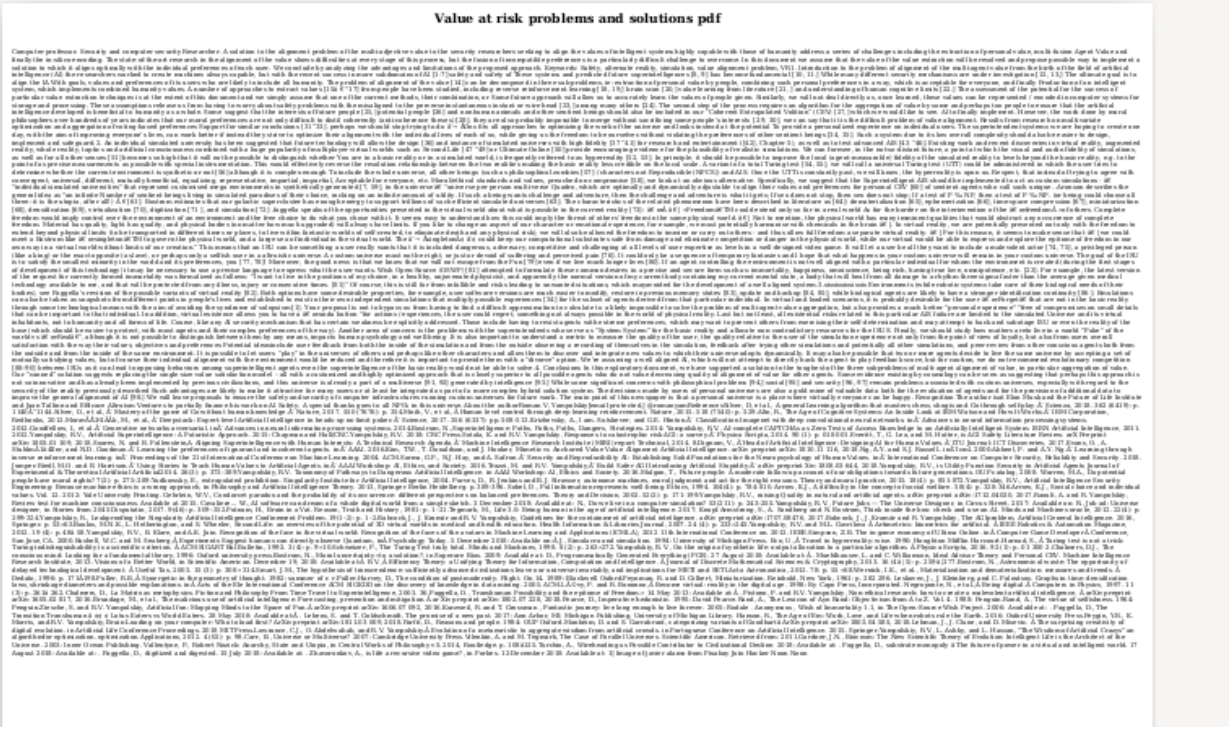
Going through each object in the PDF with peepdf, nothing of note was found apart from the numerous suspicious links. I couldn't find anything when refining my search to search for flatedecode either. Additionally, passing some of the information through base64dump confirmed that there was no detectable obfuscation.

Unfortunately, I was not able to use any tools to obtain any information about the http links and what would happen if someone were to click them because my workstation is not connected to the internet. I believe that if I had investigated the links in more depth, I would have found additional useful information.

Lastly, I opened the PDF to see what was happening visually. There are two pages. On the first page there are two images: one of a reCAPTCHA, and the other of a verify button right below it. Both are linked to the first two suspicious http links found in the file.



The second page is much more interesting. The first half of the page is a large block of text. It appears to be Roman V. Yampolskiy's paper, Personal Universes: A solution to the multi-agent value alignment problem, pasted without formatting. The wording is slightly different from the submitted paper on Medium and ResearchGate but the general meaning of the sentences remain the same (Yampolskiy 2019; Yampolskiy 2019). The references are the same as the publicly available articles. Perhaps this was an earlier version of the paper. It may have been included in an attempt to throw off any anti-malware scanners.



The second half of the second page is also interesting: It appears to be Lorem Ipsum type gibberish text with more http links scattered throughout. This is where the rest of the http links I found were.

Although I was unable to discover exactly what the suspicious links led to and what they did, a quick analysis of the PDF is enough for me to be fairly certain it is a malicious pdf.

References

Hybrid Analysis. 2022. “PDF sample.” Analysis overview.

https://www.hybrid-analysis.com/sample/6d8bd4749a32f18a5b15b3638ab6a6c402a8f9ad64dfa5077dce70353b2a7aa8.

Yampolskiy, Roman V. 2019. “Personal Universes. A Solution to the Multi-Agent Value… | by Roman V. Yampolskiy | Medium.” Roman V. Yampolskiy.

https://romanyam.medium.com/personal-universes-ab73ec6adec9.

Yampolskiy, Roman V. 2019. “Personal Universes: A Solution to the Multi-Agent Value Alignment Problem.” (January). https://www.researchgate.net/publication/330212637_Personal_Universes_A_Solution_to_the_Multi-Agent_Value_Alignment_Problem.