MalDoc in PDF - Detection bypass by embedding a malicious Word file into a PDF file –

blogs.jpcert.or.jp/en/2023/08/maldocinpdf.html

増渕 維摩(Yuma Masubuchi)

August 28, 2023

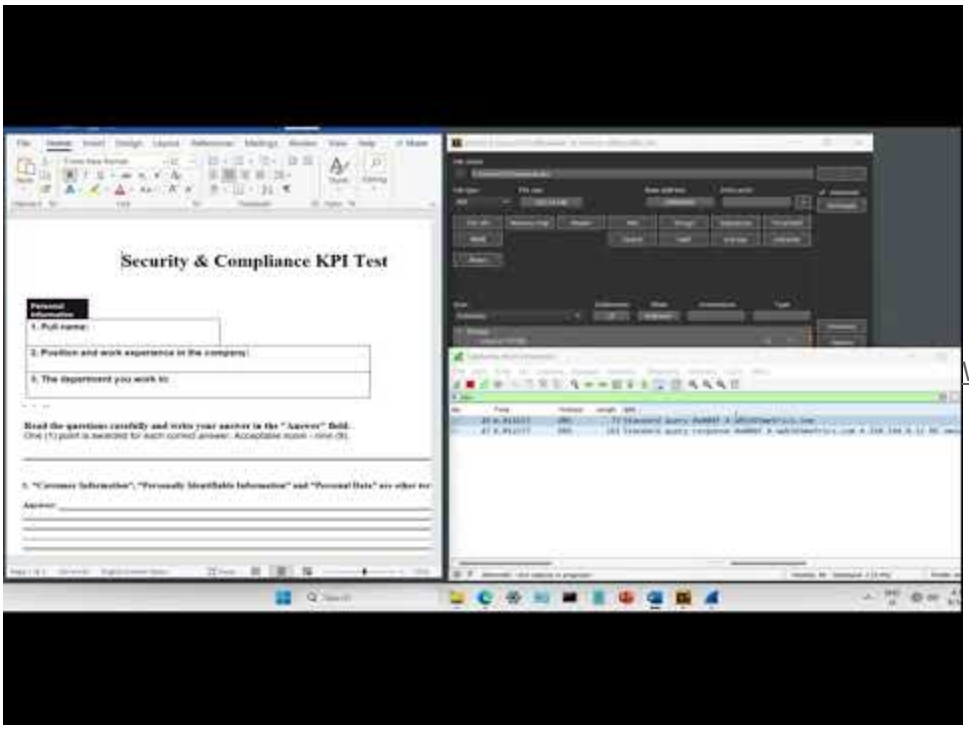
-
- Email

JPCERT/CC has confirmed that a new technique was used in an attack that occurred in July, which bypasses detection by embedding a malicious Word file into a PDF file. This blog article calls the technique “MalDoc in PDF” hereafter and explains the details of and countermeasures against it.

Overview of MalDoc in PDF

A file created with MalDoc in PDF can be opened in Word even though it has magic numbers and file structure of PDF. If the file has configured macro, by opening it in Word, VBS runs and performs malicious behaviors. In the attack confirmed by JPCERT/CC, the file extension was .doc. Therefore, if a .doc file is configured to open in Word in Windows settings, the file created by MalDoc in PDF is opened as a Word file.

Please watch the below video of this technique, from opening the created file in Word until the communication occurs.

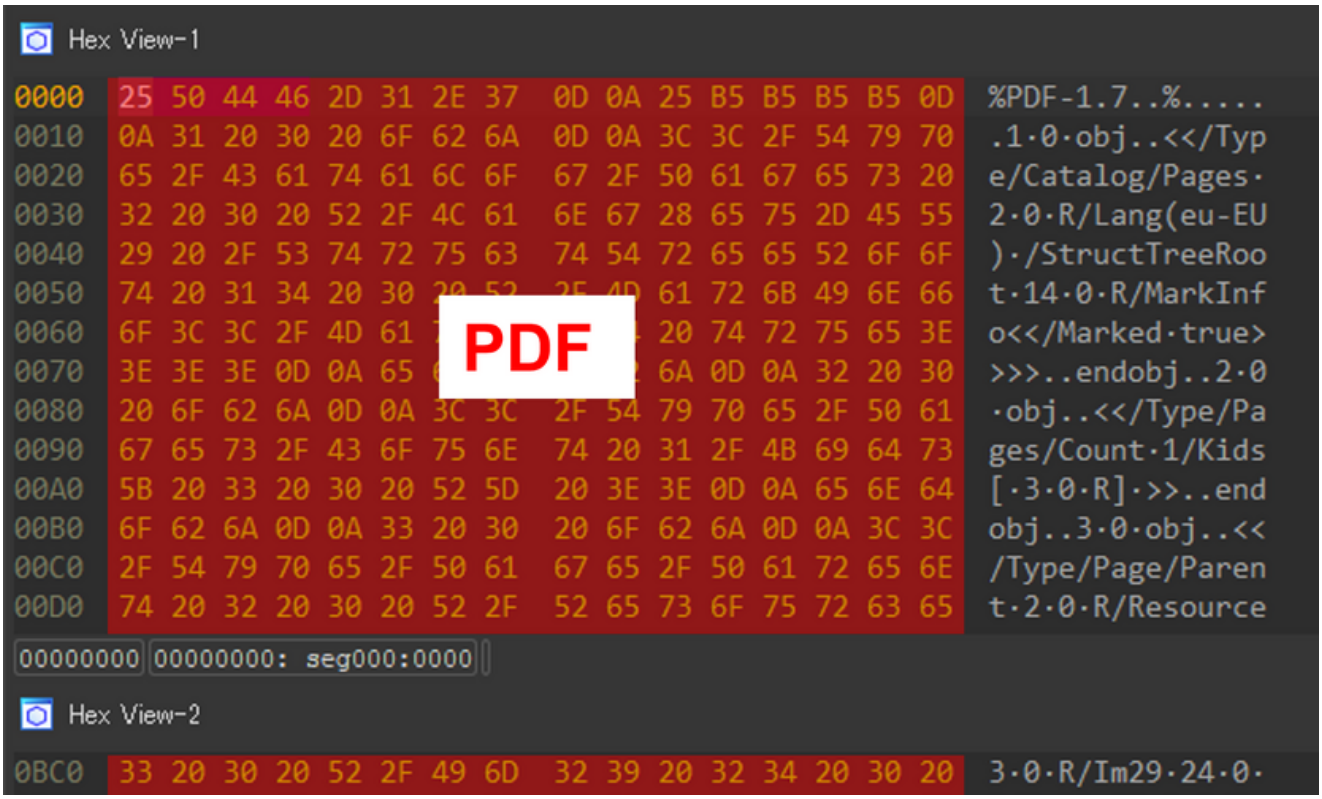


Watch Video At:

https://youtu.be/mlx_chLuVCI

Details of MalDoc in PDF

Figure 1 shows the dump view of the file created by this technique. The attacker adds an mht file created in Word and with macro attached after the PDF file object and saves it. The created file is recognized as a PDF file in the file signature, but it can also be opened in Word.



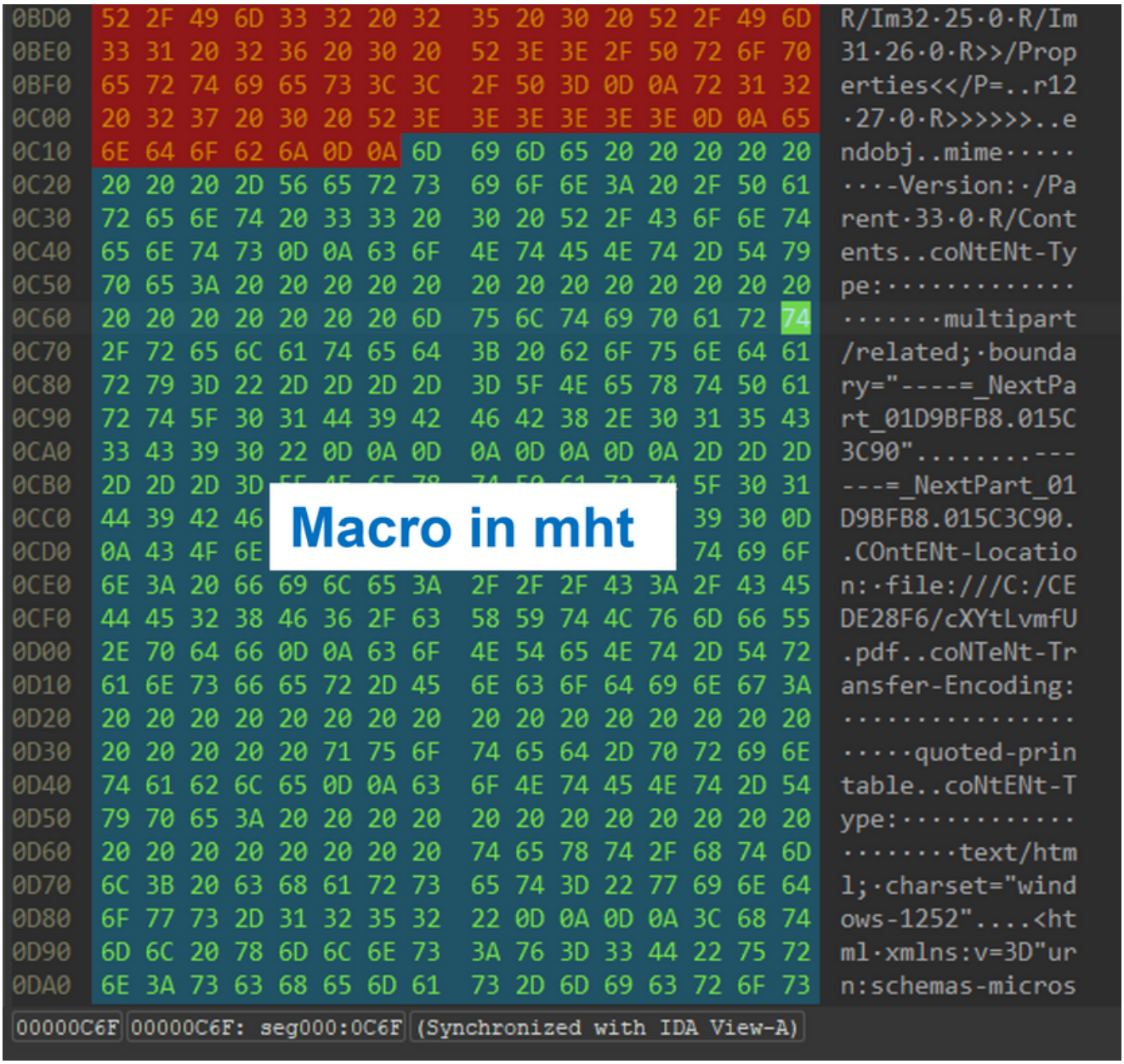


Figure 1: Dump view of MalDoc in PDF

When analyzing a file created with MalDoc in PDF, there is a high possibility that PDF analysis tools such as pdfid[1] cannot detect its malicious parts, as shown in Figure 2. In addition, it should be noted that this file performs unintentional behaviors when opened in Word, while malicious behaviors cannot be confirmed when it is opened in PDF viewers, etc. Furthermore, since the file is recognized as a PDF file, existing sandbox or antivirus software may not detect it.

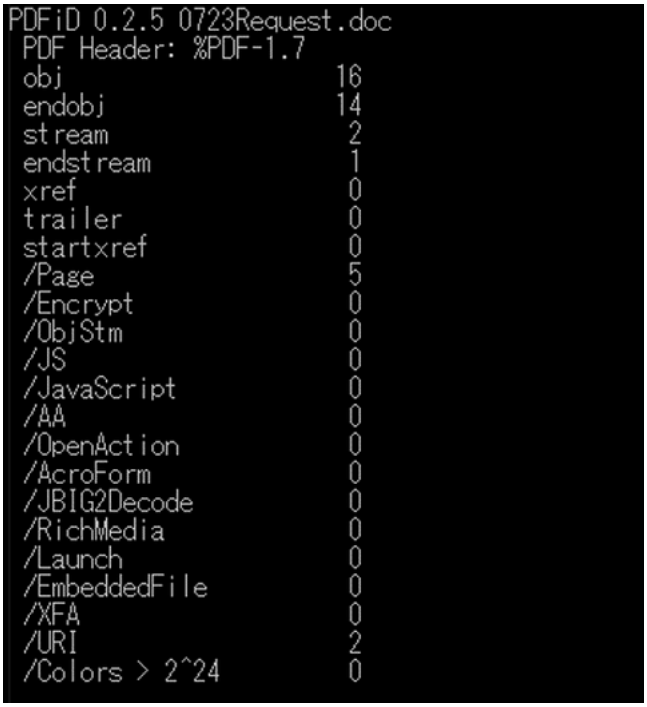


Figure 2: pdfid’s analysis results

Countermeasures against MalDoc in PDF

OLEVBA [2], an analysis tool for malicious Word files, is still an effective countermeasure to this technique. As shown in Figure 3, OLEVBA outputs the embedded macros, and thus the malicious parts of the file can be checked with the tool's analysis results.

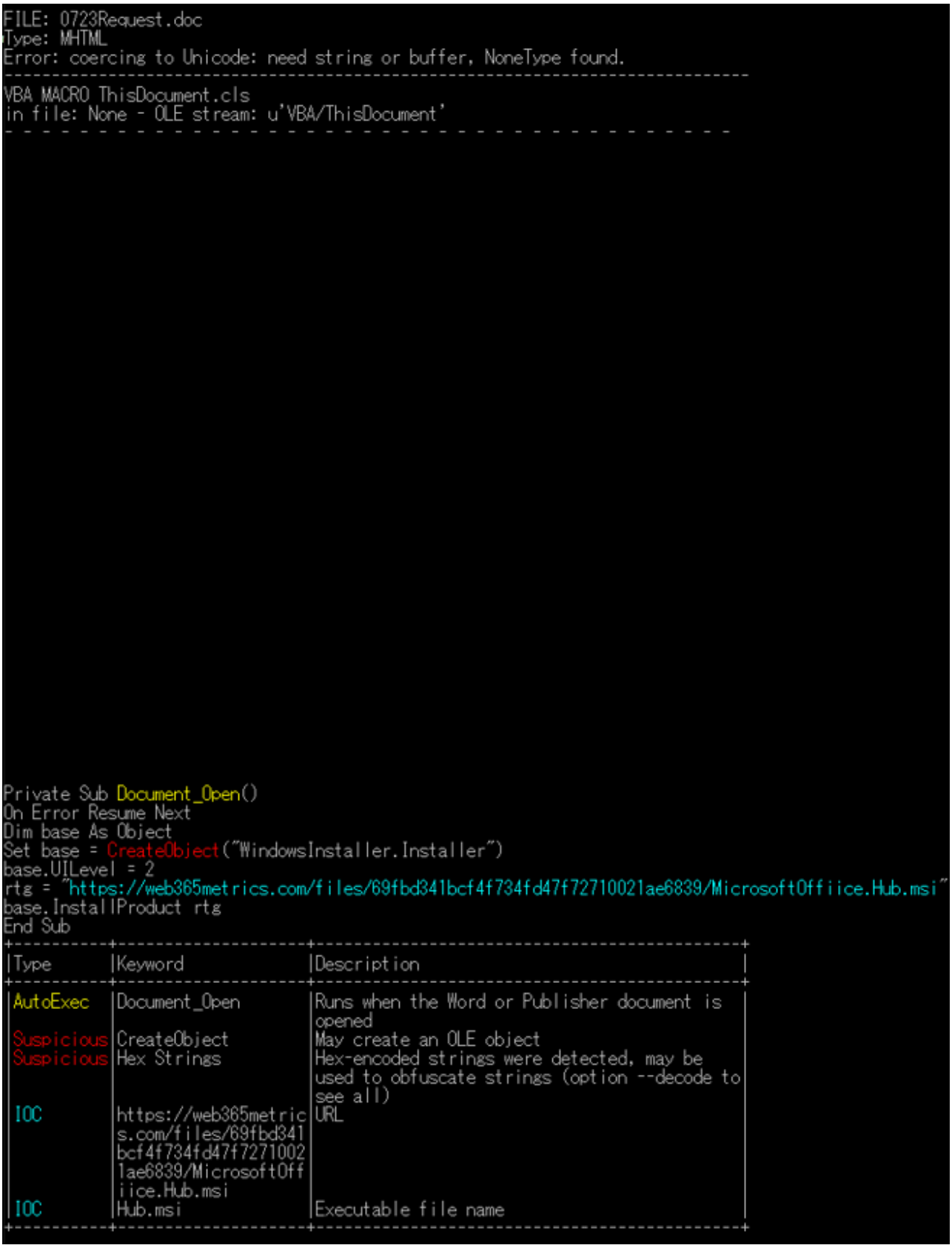


Figure 3: OLEVBA's analysis results

The below is an example of a detection rule created using Yara rule. In this method, if an Excel file is stored in a PDF file, a warning screen is displayed when Excel starts up, stating that the file extension is different, and the file will not be opened in Excel unless the warning is accepted. Therefore, at the time of the release of this article, it is unlikely that Excel files are used for this technique.

```
rule malware_MaldocinPDF {

    strings:
        $docfile2 = "<w:WordDocument>" ascii nocase
        $xlsfile2 = "<x:ExcelWorkbook>" ascii nocase
        $mhtfile0 = "mime" ascii nocase
        $mhtfile1 = "content-location:" ascii nocase
        $mhtfile2 = "content-type:" ascii nocase

     condition:
        (uint32(0) == 0x46445025) and
        (1 of ($mhtfile*)) and
        ( (1 of ($docfile*)) or
          (1 of ($xlsfile*)) )
}
```

In Closing

The technique described in this article does not bypass the setting that disables auto-execution in Word macro. However, since the files are recognized as PDFs, you should be careful about the detection results if you are performing automated malware analysis using some tools, sandbox, etc. Please refer to the Appendix for the C2 information and hash values of the confirmed malware.

Yuma Masubuchi and Kota Kino

(Translated by Takumi Nakano)

References

[1] pdfid.py
https://github.com/DidierStevens/DidierStevensSuite/blob/master/pdfid.py

[2] OLEVBA
https://github.com/decalage2/oletools/wiki/olevba

Appendix A: C2 information

- https[:]//cloudmetricsapp[.]com
- https[:]//web365metrics[.]com

Appendix B: Malware hash value

- ef59d7038cfd565fd65bae12588810d5361df938244ebad33b71882dcf683058
- 098796e1b82c199ad226bff056b6310262b132f6d06930d3c254c57bdf548187
- 5b677d297fb862c2d223973697479ee53a91d03073b14556f421b3d74f136b9d

-
- Email

Author

増渕 維摩(Yuma Masubuchi)

Yuma has been engaged in malware analysis and coordination of cyber security incidents in JPCERT/CC Incident Response Group since November 2020.

Was this page helpful?

0 people found this content helpful.

If you wish to make comments or ask questions, please use this form.

This form is for comments and inquiries. For any questions regarding specific commercial products, please contact the vendor.

please change the setting of your browser to set JavaScript valid. Thank you!

Back
Top