Analysis of document "The Incident Response Field Guide"

Objective: To determine if file is malicious

Delivery method: USB Flash Drive – SanDisk 32GB – Colors: black & red

Tools:

- WinMD5 Free v1.20
- Virus Total
- Bintext
- Minidumpt
- GT2
- Jotti
- Virscan
- IDA Pro

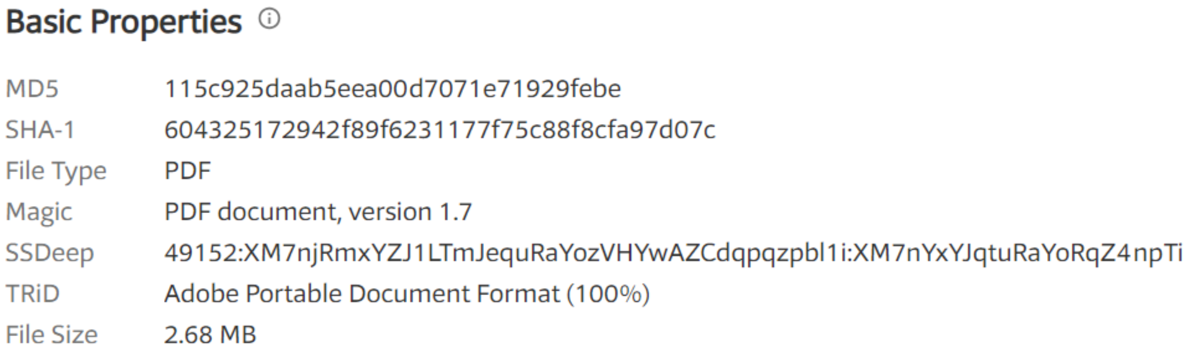
File Information:

- MD5 Checksum: 115c925daab5eea00d7071e71929febe
- SHA-256: bc2fb7aeceb6b1e8860ebb8164e1d31a934070478506893c2d811ffbfc3acd4a
- Size: 2.67 MB
- Created: February 3, 2019
- Last Modified: February 3, 2019
- File Type: PDF
- Computer document was created on: XXXXCHANDS59L1C

Method:

Got MD5 hash of the file

Checked to see if hash matched any known specimens of malicious files on Virus Total and Threat Expert



Basic Properties

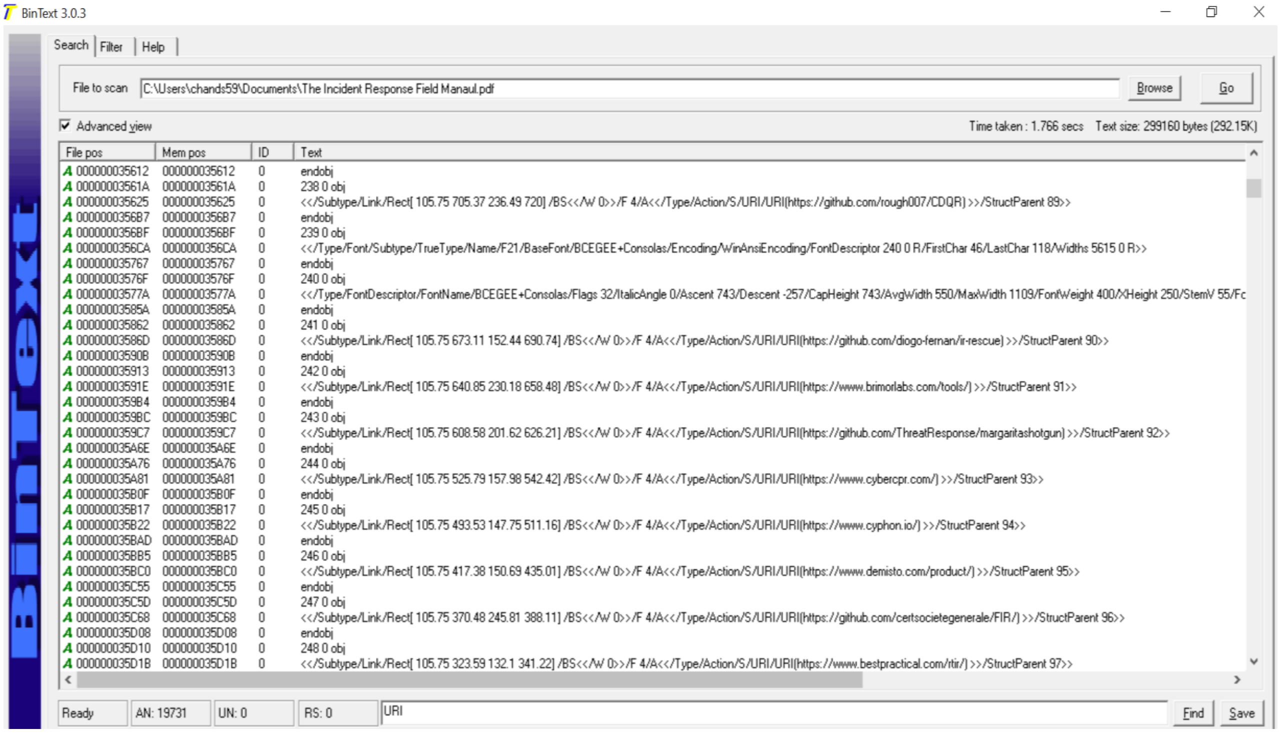
MD5	115c925daab5eea00d7071e71929febe
SHA-1	604325172942f89f6231177f75c88f8cfa97d07c
File Type	PDF
Magic	PDF document, version 1.7
SSDeep	49152:XM7njRmxYZJ1LTmJequRaYozVHYwAZCdqpqzpbl1i:XM7nYxYJqtuRaYoRqZ4npTi
TRiD	Adobe Portable Document Format (100%)
File Size	2.68 MB

Tools- Minidumper and GT2

Scanned file with Antivirus

- McAfee, Virus Total, Virscan, Jotti

Using bintext I see multiple links to sites such as Github, and Webopedia.



File to scan: C:\Users\chands59\Documents\The Incident Response Field Manaul.pdf

☑ Advanced view

Time taken : 1.766 secs   Text size: 299160 bytes (292.15K)

```
File pos       Mem pos        ID  Text
A 000000035612 000000035612   0   endobj
A 00000003561A 00000003561A   0   238 0 obj
A 000000035625 000000035625   0   <</Subtype/Link/Rect[ 105.75 705.37 236.49 720] /BS<</W 0>>/F 4/A<</Type/Action/S/URI/URI(https://github.com/rough007/CDQR) >>/StructParent 89>>
A 0000000356B7 0000000356B7   0   endobj
A 0000000356BF 0000000356BF   0   239 0 obj
A 0000000356CA 0000000356CA   0   <</Type/Font/Subtype/TrueType/Name/F21/BaseFont/BCEGEE+Consolas/Encoding/WinAnsiEncoding/FontDescriptor 240 0 R/FirstChar 46/LastChar 118/Widths 5615 0 R>>
A 000000035767 000000035767   0   endobj
A 00000003576F 00000003576F   0   240 0 obj
A 00000003577A 00000003577A   0   <</Type/FontDescriptor/FontName/BCEGEE+Consolas/Flags 32/ItalicAngle 0/Ascent 743/Descent -257/CapHeight 743/AvgWidth 550/MaxWidth 1109/FontWeight 400/XHeight 250/StemV 55/Fc
A 00000003585A 00000003585A   0   endobj
A 000000035862 000000035862   0   241 0 obj
A 00000003586D 00000003586D   0   <</Subtype/Link/Rect[ 105.75 673.11 152.44 690.74] /BS<</W 0>>/F 4/A<</Type/Action/S/URI/URI(https://github.com/diogo-fernan/ir-rescue) >>/StructParent 90>>
A 00000003590B 00000003590B   0   endobj
A 000000035913 000000035913   0   242 0 obj
A 00000003591E 00000003591E   0   <</Subtype/Link/Rect[ 105.75 640.85 230.18 658.48] /BS<</W 0>>/F 4/A<</Type/Action/S/URI/URI(https://www.brimorlabs.com/tools/) >>/StructParent 91>>
A 0000000359B4 0000000359B4   0   endobj
A 0000000359BC 0000000359BC   0   243 0 obj
A 0000000359C7 0000000359C7   0   <</Subtype/Link/Rect[ 105.75 608.58 201.62 626.21] /BS<</W 0>>/F 4/A<</Type/Action/S/URI/URI(https://github.com/ThreatResponse/margaritashotgun) >>/StructParent 92>>
A 000000035A6E 000000035A6E   0   endobj
A 000000035A76 000000035A76   0   244 0 obj
A 000000035A81 000000035A81   0   <</Subtype/Link/Rect[ 105.75 525.79 157.98 542.42] /BS<</W 0>>/F 4/A<</Type/Action/S/URI/URI(https://www.cybercpr.com/) >>/StructParent 93>>
A 000000035B0F 000000035B0F   0   endobj
A 000000035B17 000000035B17   0   245 0 obj
A 000000035B22 000000035B22   0   <</Subtype/Link/Rect[ 105.75 493.53 147.75 511.16] /BS<</W 0>>/F 4/A<</Type/Action/S/URI/URI(https://www.cyphon.io/) >>/StructParent 94>>
A 000000035BAD 000000035BAD   0   endobj
A 000000035BB5 000000035BB5   0   246 0 obj
A 000000035BC0 000000035BC0   0   <</Subtype/Link/Rect[ 105.75 417.38 150.69 435.01] /BS<</W 0>>/F 4/A<</Type/Action/S/URI/URI(https://www.demisto.com/product/) >>/StructParent 95>>
A 000000035C55 000000035C55   0   endobj
A 000000035C5D 000000035C5D   0   247 0 obj
A 000000035C68 000000035C68   0   <</Subtype/Link/Rect[ 105.75 370.48 245.81 388.11] /BS<</W 0>>/F 4/A<</Type/Action/S/URI/URI(https://github.com/certsocietegenerale/FIR/) >>/StructParent 96>>
A 000000035D08 000000035D08   0   endobj
A 000000035D10 000000035D10   0   248 0 obj
A 000000035D1B 000000035D1B   0   <</Subtype/Link/Rect[ 105.75 323.59 132.1 341.22] /BS<</W 0>>/F 4/A<</Type/Action/S/URI/URI(https://www.bestpractical.com/rtir/) >>/StructParent 97>>
```

```
Ready | AN: 19731 | UN: 0 | RS: 0 | URI
```

No unusual services or process started after opening file.

- Used IDA Pro

No changes to registry keys.

Checked to see if the following had been modified:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx

Scanned for any newly created files.

Conclusion:

File is not malicious