

Maldocs: Tips for Red Teamers

Pen Test HackFest & Cyber Ranges Summit

- 1** Quick intro Office file format
- 2** 4 tips for red teamers
- 3** Examples (with some disclosures)
- 4** Questions



Didier Stevens

Senior Analyst, SANS ISC Senior Handler

dstevens@nviso.eu



Quick intro Office file format

Maldocs: Tips for Red Teamers



OOXML: Office Open XML

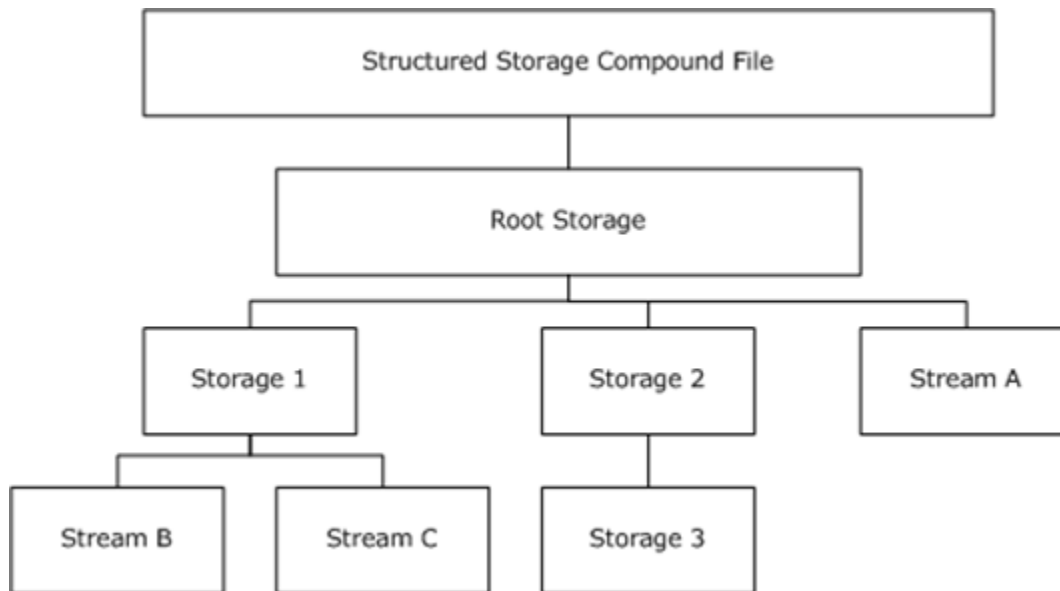
ZIP + XMLs (+ sometimes a bit more)

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

CFBF: Compound File Binary Format

I like to call this OLE format

.doc, .xls, ...





4 tips for red teamers

4 tips for red teamers

1

Analyze your `sh+chr(105)+t`

4 tips for red teamers

1 Analyze your `sh+chr(105)+t`

2 Learn from actors

4 tips for red teamers

1 Analyze your `sh+chr(105)+t`

2 Learn from actors

3 RTFM & use it

4 tips for red teamers

1 Analyze your `sh+chr(105)+t`

2 Learn from actors

3 RTFM & use it

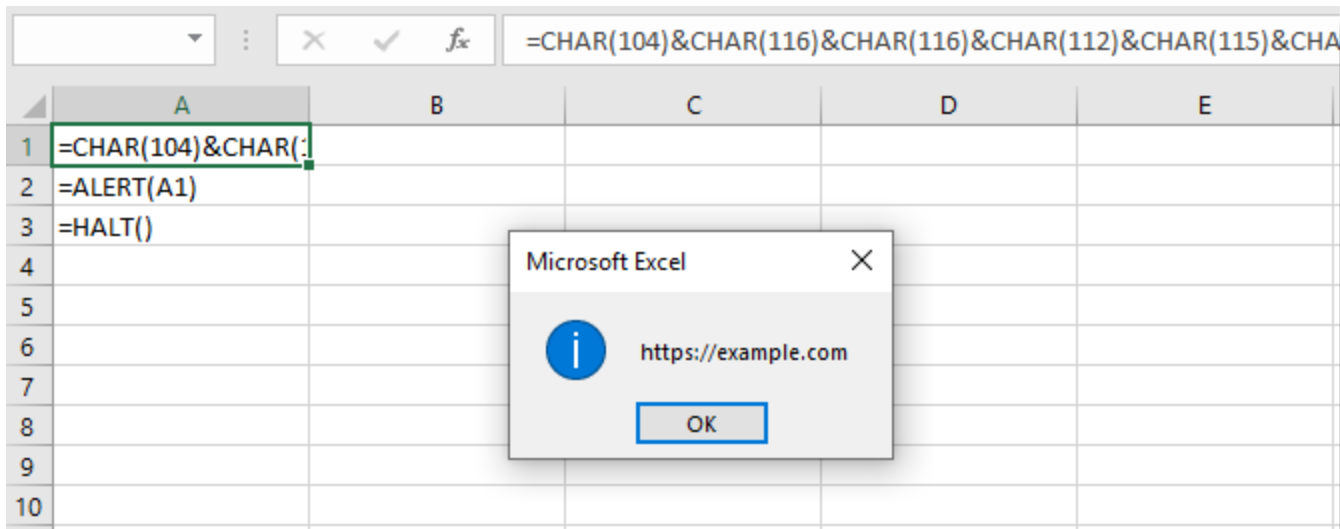
4 RTFM & abuse it



Examples (with some disclosures)

Example 1: the power of strings

Tip 1: Analyze!



Example 1: the power of strings

Tip 1: Analyze!

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

@NVISOLabs C:\Demo>
```


Example 1: the power of strings

Tip 1: Analyze!



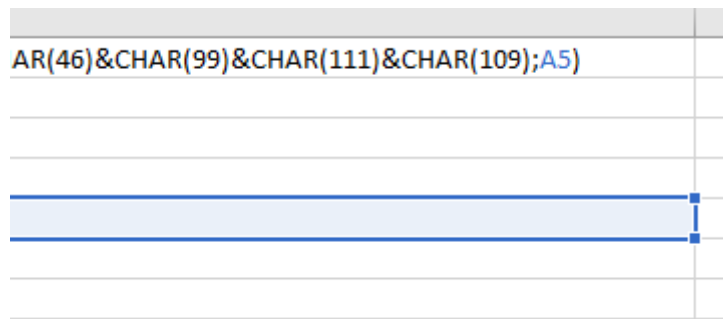
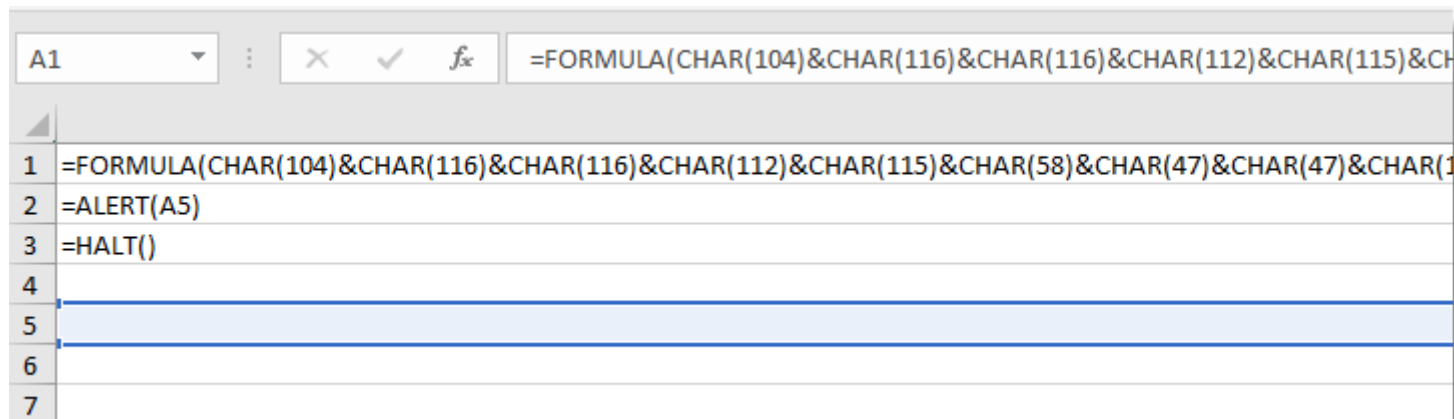
```
@NVIISO_Labs C:\Demo>oledump.py example-01.xls
1:      4096 '\x05DocumentSummaryInformation'
2:      4096 '\x05SummaryInformation'
3:     16331 'Workbook'

@NVIISO_Labs C:\Demo>oledump.py -y #s#http example-01.xls
1:      4096 '\x05DocumentSummaryInformation'
2:      4096 '\x05SummaryInformation'
3:     16331 'Workbook'
          YARA rule: string

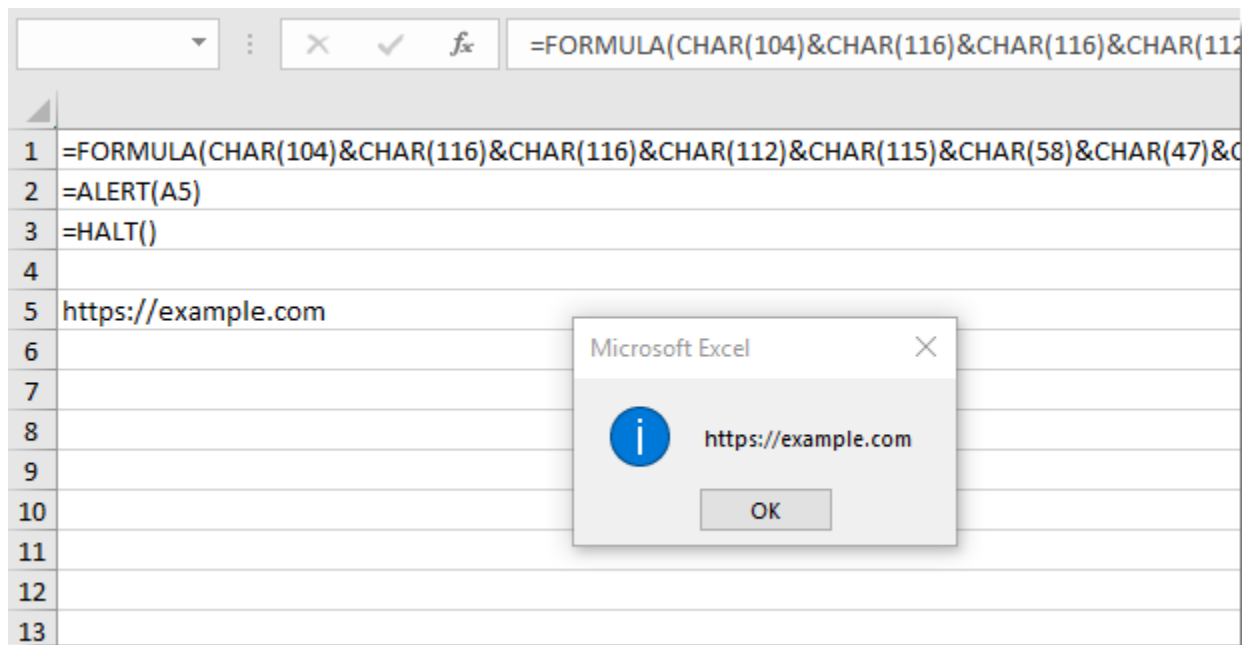
@NVIISO_Labs C:\Demo>
```

Example 2: limiting the power of strings

Tip 2: Learn!



Tip 2: Learn!



Example 2: limiting the power of strings

Tip 2: Learn!



```
C:\> @NVISO_Labs

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

@NVISO_Labs C:\Demo>
```

Example 2: limiting the power of strings

Tip 2: Learn!



```
@NVISO_Labs C:\Demo>oledump.py -p plugin_biff --pluginoptions "-c" example-02.xls
1:      4096 '\x05DocumentSummaryInformation'
2:      4096 '\x05SummaryInformation'
3:     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(
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>
```

Example 2: limiting the power of strings

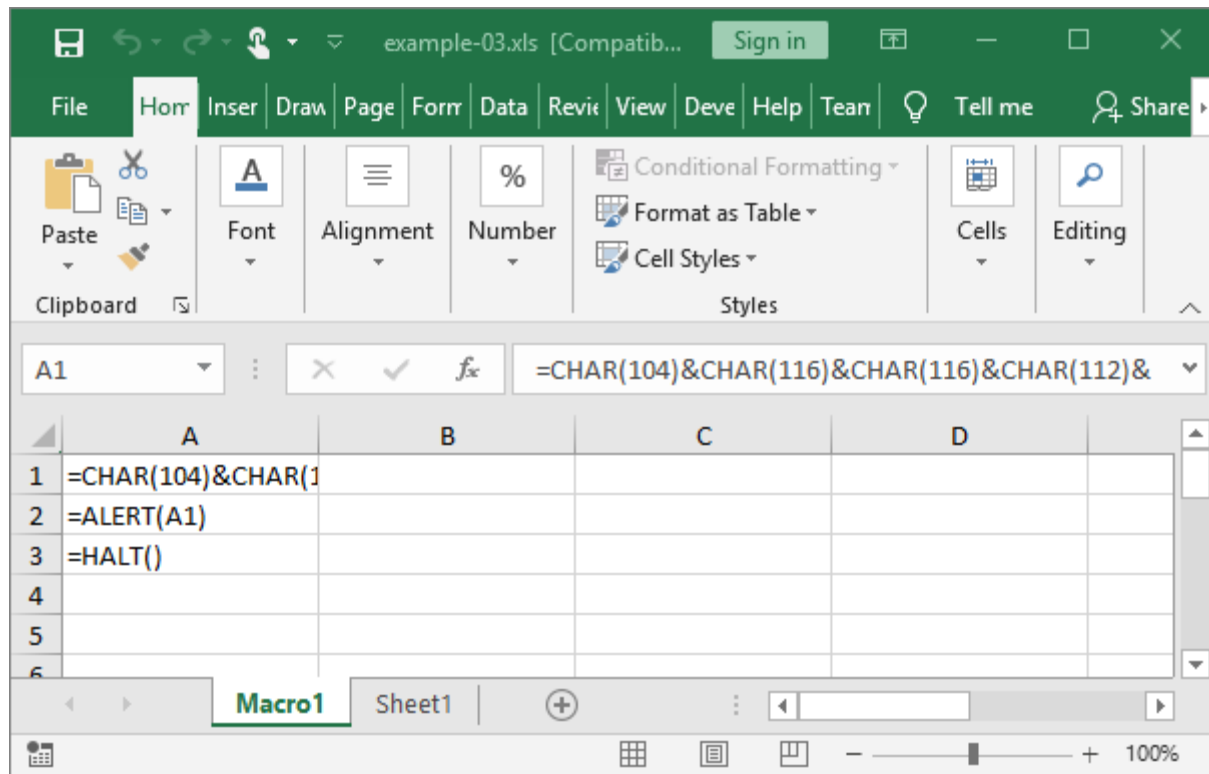
Tip 2: Learn!



```
@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>
```

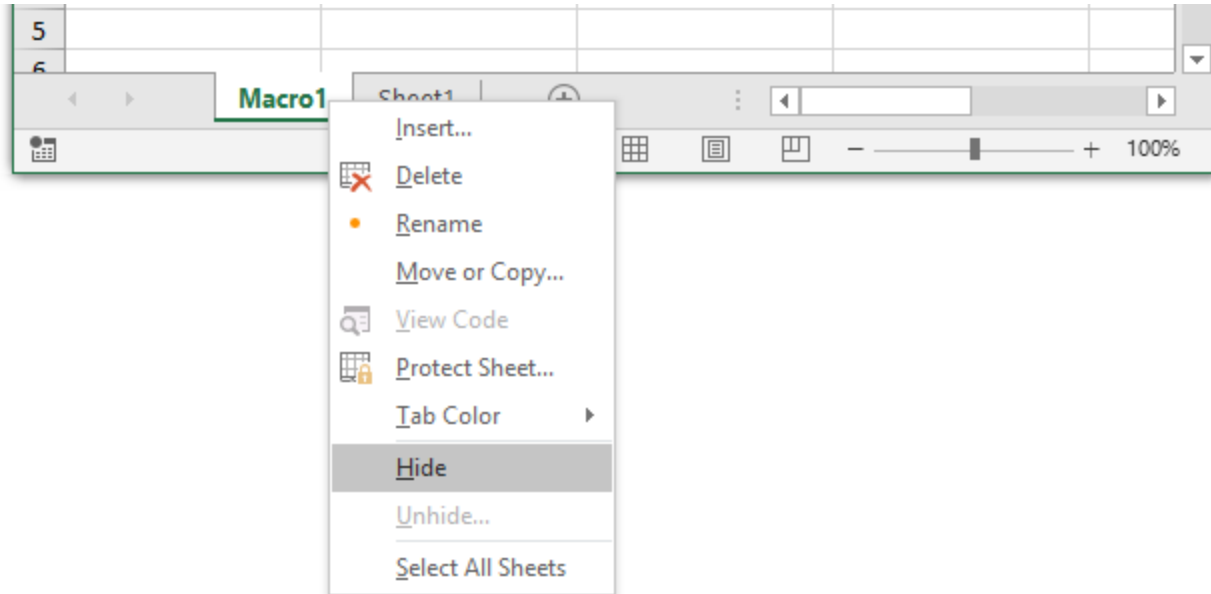
Example 3: very hidden

Tip 3: Use!



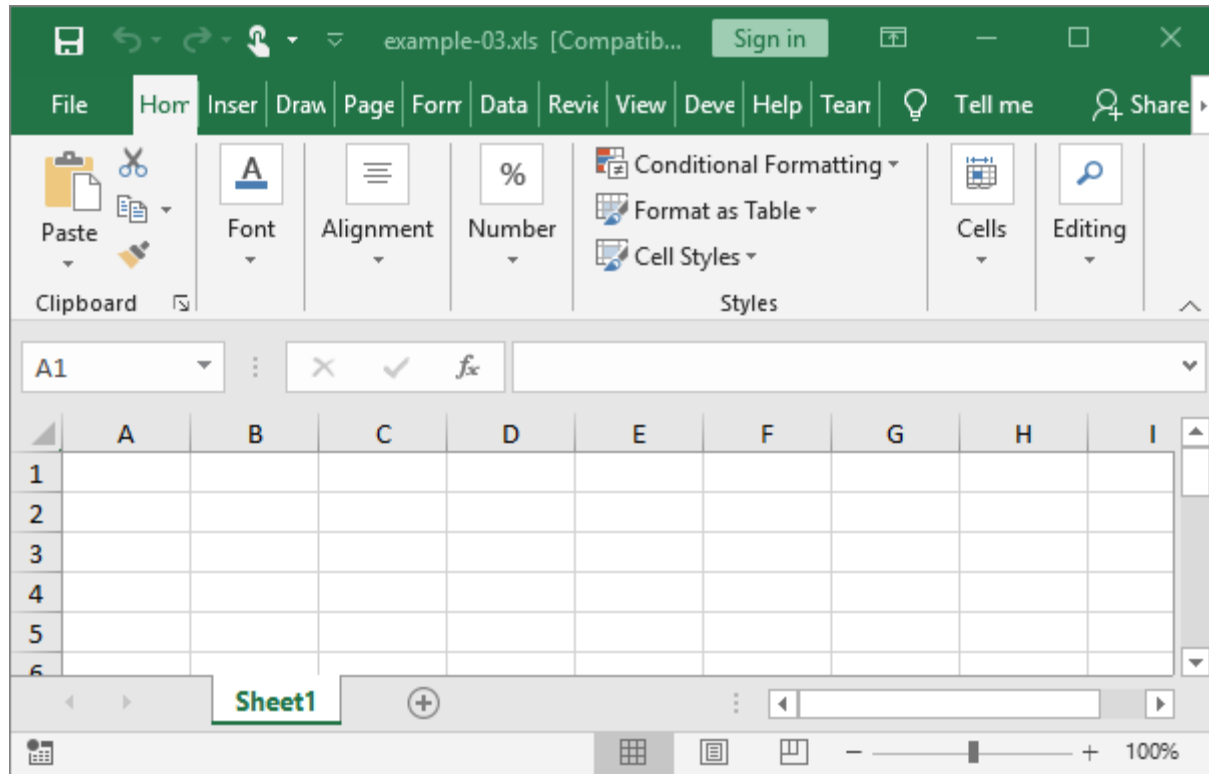
Example 3: very hidden

Tip 3: Use!



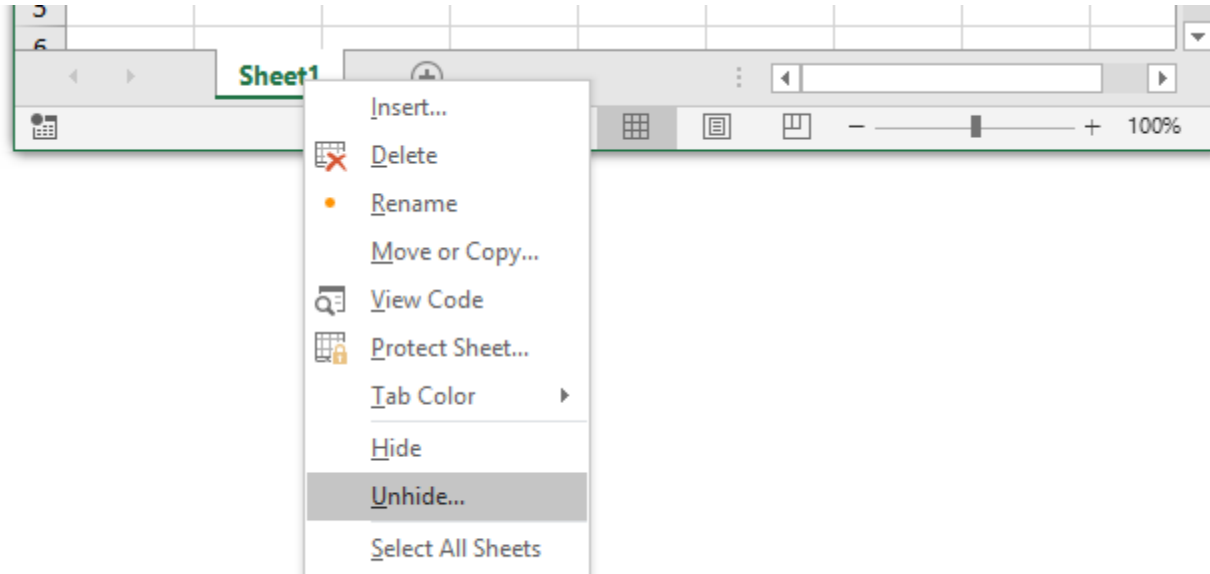
Example 3: very hidden

Tip 3: Use!



Example 3: very hidden

Tip 3: Use!



Example 3: very hidden

Tip 3: Use!



```
@NVISO_Labs C:\Demo>oledump.py -p plugin_biff --pluginoptions "-o BOUNDSHEET" example-03.xls
1:      4096 '\x05DocumentSummaryInformation'
2:      4096 '\x05SummaryInformation'
3:     16331 'Workbook'
        Plugin: BIFF plugin
        0085      14 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden - Macro1
        0085      14 BOUNDSHEET : Sheet Information - worksheet or dialog sheet, visible - Sheet1

@NVISO_Labs C:\Demo>
```

Example 3: very hidden

Tip 3: Use!



```
@Nviso_Labs C:\Demo>oledump.py -p plugin_biff --pluginoptions "-o BOUNDSHEET -a" example-03.xls
1:      4096 '\x05DocumentSummaryInformation'
2:      4096 '\x05SummaryInformation'
3:     16331 'Workbook'
      Plugin: BIFF plugin
      0085      14 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden - Macro1
      00000000: 68 3B 00 00 01 01 06 00  h;.....
      00000008: 4D 61 63 72 6F 31      Macro1
      0085      14 BOUNDSHEET : Sheet Information - worksheet or dialog sheet, visible - Sheet1
      00000000: 45 3E 00 00 00 00 06 00  E>.....
      00000008: 53 68 65 65 74 31      Sheet1

@Nviso_Labs C:\Demo>
```

Example 3: very hidden

Tip 3: Use!

2.4.28 BoundSheet8

The **BoundSheet8** record specifies basic information about a **sheet (1)**, including the sheet (1) name, **hidden** state, and type of sheet (1).

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
lbPlyPos																															
A		unused						dt				stName (variable)																			
...																															

lbPlyPos (4 bytes): A FilePointer as specified in [\[MS-OSHARED\]](#) section 2.2.1.5 that specifies the stream position of the start of the [BOF](#) record for the sheet (1).

A - hsState (2 bits): An unsigned integer that specifies the hidden state of the sheet (1). MUST be a value from the following table:

Value	Meaning
0x00	Visible
0x01	Hidden
0x02	Very Hidden; the sheet (1) is hidden and cannot be displayed using the user interface.

unused (6 bits): Undefined and MUST be ignored.

Example 3: very hidden

Tip 3: Use!

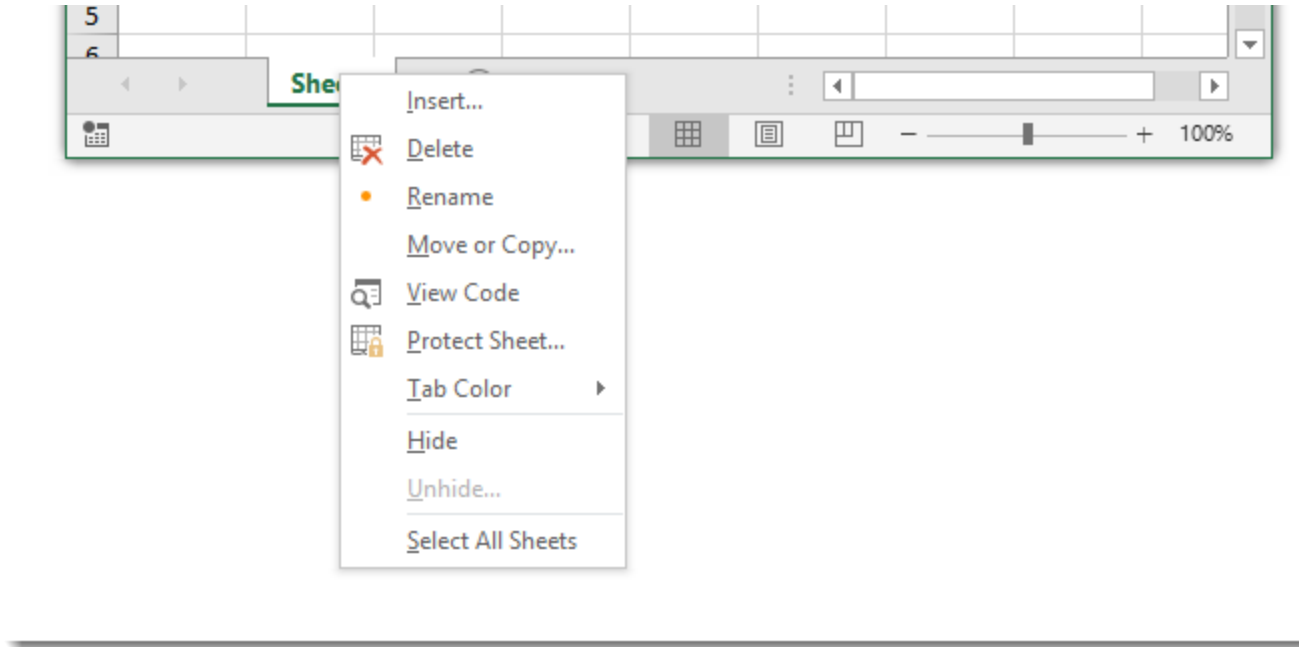


```
@Nviso_Labs C:\Demo>oledump.py -p plugin_biff --pluginoptions "-o BOUNDSHEET -a" example-03b.xls
1:      4096 '\x05DocumentSummaryInformation'
2:      4096 '\x05SummaryInformation'
3:     16331 'Workbook'
      Plugin: BIFF plugin
      0085      14 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, very hidden - Macro1
      00000000: 68 3B 00 00 02 01 06 00  h;.....
      00000008: 4D 61 63 72 6F 31          Macro1
      0085      14 BOUNDSHEET : Sheet Information - worksheet or dialog sheet, visible - Sheet1
      00000000: 45 3E 00 00 00 00 06 00  E>.....
      00000008: 53 68 65 65 74 31          Sheet1

@Nviso_Labs C:\Demo>
```

Example 3: very hidden

Tip 3: Use!



Example 4: very, very hidden?

Tip 4: Abuse!

2.4.28 BoundSheet8

The **BoundSheet8** record specifies basic information about a **sheet (1)**, including the sheet (1) name, **hidden** state, and type of sheet (1).

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
lbPlyPos																															
A	unused					dt					stName (variable)																				
...																															

lbPlyPos (4 bytes): A FilePointer as specified in [\[MS-OSHARED\]](#) section 2.2.1.5 that specifies the stream position of the start of the [BOF](#) record for the sheet (1).

A - hsState (2 bits): An unsigned integer that specifies the hidden state of the sheet (1). MUST be a value from the following table:

Value	Meaning
0x00	Visible
0x01	Hidden
0x02	Very Hidden; the sheet (1) is hidden and cannot be displayed using the user interface.

unused (6 bits): Undefined and MUST be ignored.

Example 4: very, very hidden?

Tip 4: Abuse!



```
@NVISO_Labs C:\Demo>oledump.py -p plugin_biff --pluginoptions "-o BOUNDSHEET -a" example-04.xls
```

```
1:      4096 '\x05DocumentSummaryInformation'
```

```
2:      4096 '\x05SummaryInformation'
```

```
3:     16331 'Workbook'
```

```
    Plugin: BIFF plugin
```

```
    0085      14 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, visibility=3 - Macro1
```

```
    00000000: 68 3B 00 00 03 01 06 00 h;.....
```

```
    00000008: 4D 61 63 72 6F 31      Macro1
```

```
    0085      14 BOUNDSHEET : Sheet Information - worksheet or dialog sheet, visible - Sheet1
```

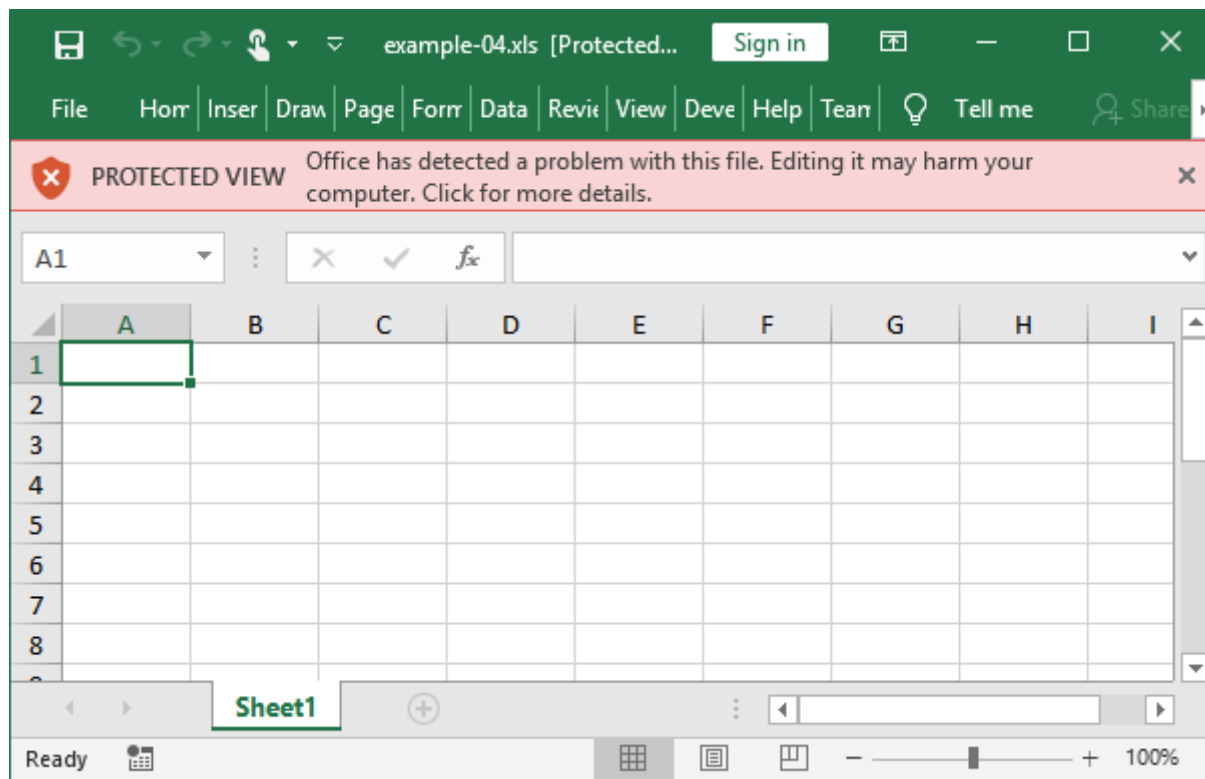
```
    00000000: 45 3E 00 00 00 00 06 00 E>.....
```

```
    00000008: 53 68 65 65 74 31      Sheet1
```

```
@NVISO_Labs C:\Demo>
```

Example 4: very, very hidden?

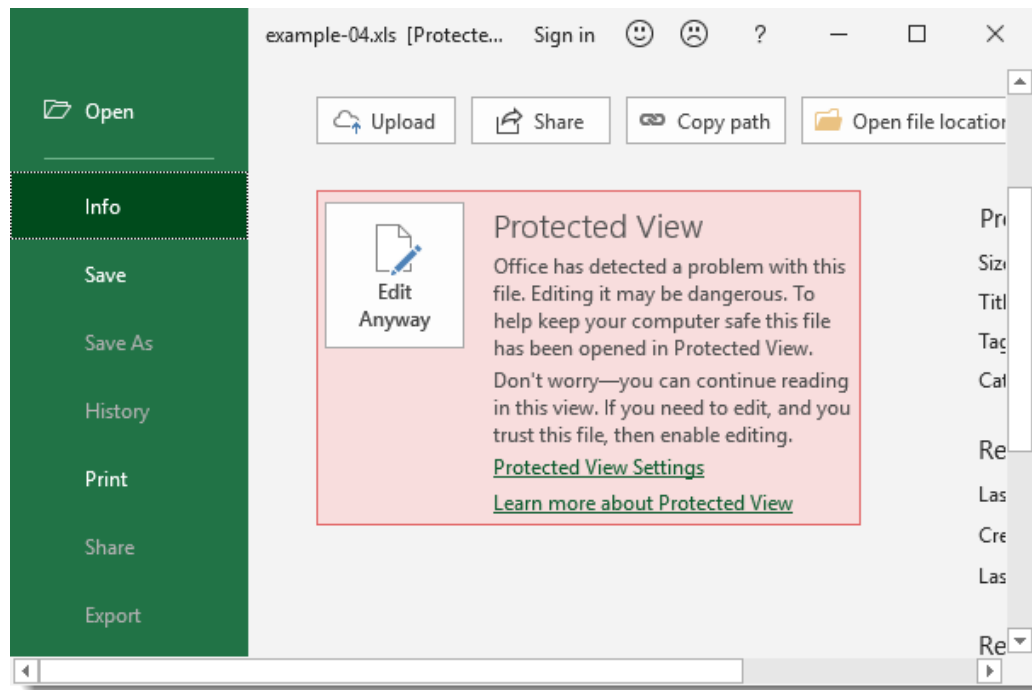
Tip 4: Abuse!



Disclosure

Example 4: very, very hidden?

Tip 4: Abuse!



Example 5: unused bits

Tip 4: Abuse!

2.4.28 BoundSheet8

The **BoundSheet8** record specifies basic information about a **sheet (1)**, including the sheet (1) name, **hidden** state, and type of sheet (1).

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
lbPlyPos																															
A	unused					dt					stName (variable)																				
...																															

lbPlyPos (4 bytes): A FilePointer as specified in [\[MS-OSHARED\]](#) section 2.2.1.5 that specifies the stream position of the start of the [BOF](#) record for the sheet (1).

A - hsState (2 bits): An unsigned integer that specifies the hidden state of the sheet (1). MUST be a value from the following table:

Value	Meaning
0x00	Visible
0x01	Hidden
0x02	Very Hidden; the sheet (1) is hidden and cannot be displayed using the user interface.

unused (6 bits): Undefined and MUST be ignored.

Example 5: unused bits

Tip 4: Abuse!

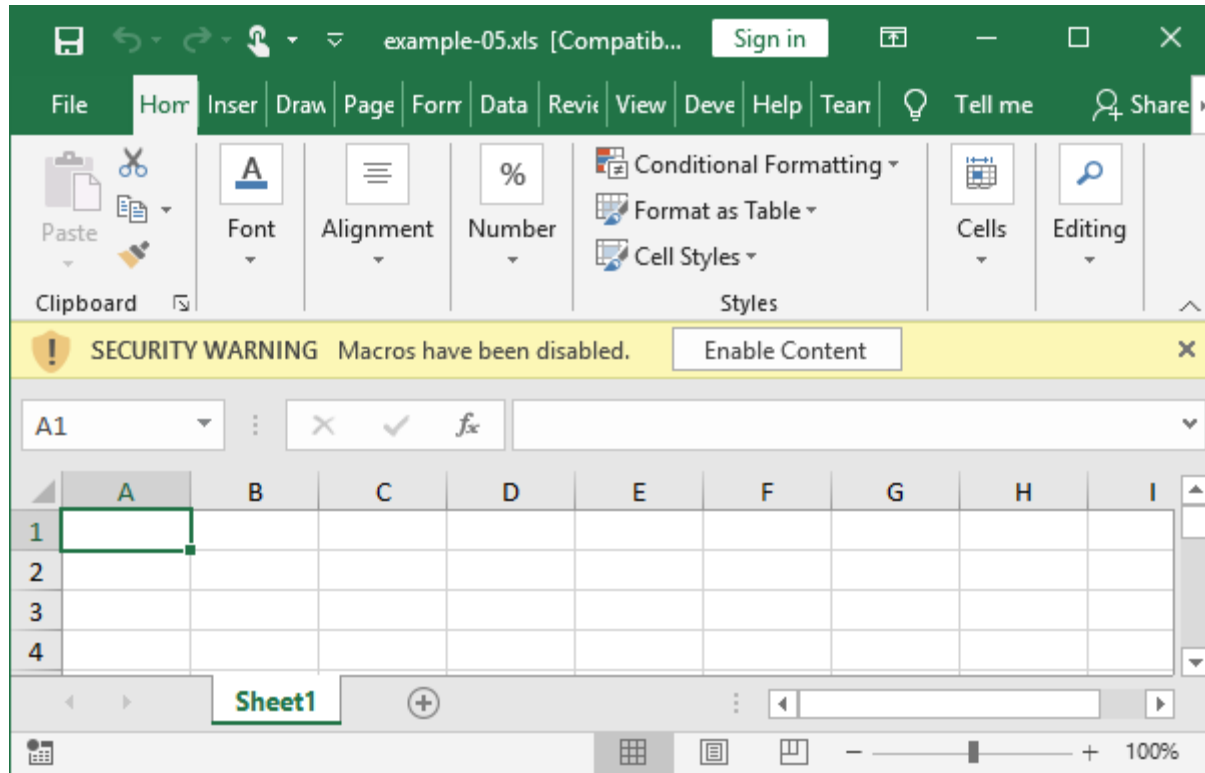


```
@Nviso_Labs C:\Demo>oledump.py -p plugin_biff --pluginoptions "-o BOUNDSHEET -a" example-05.xls
1:      4096 '\x05DocumentSummaryInformation'
2:      4096 '\x05SummaryInformation'
3:     16358 'Workbook'
      Plugin: BIFF plugin
      0085      14 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, reserved bits not zero: 0x10 very h
idden - Macro1
      ' 00000000: 83 3B 00 00 12 01 06 00  \x83;.....'
      00000008: 4D 61 63 72 6F 31      Macro1
      0085      14 BOUNDSHEET : Sheet Information - worksheet or dialog sheet, visible - Sheet1
      00000000: 60 3E 00 00 00 00 06 00  `>.....
      00000008: 53 68 65 65 74 31      Sheet1

@Nviso_Labs C:\Demo>
```

Example 5: unused bits

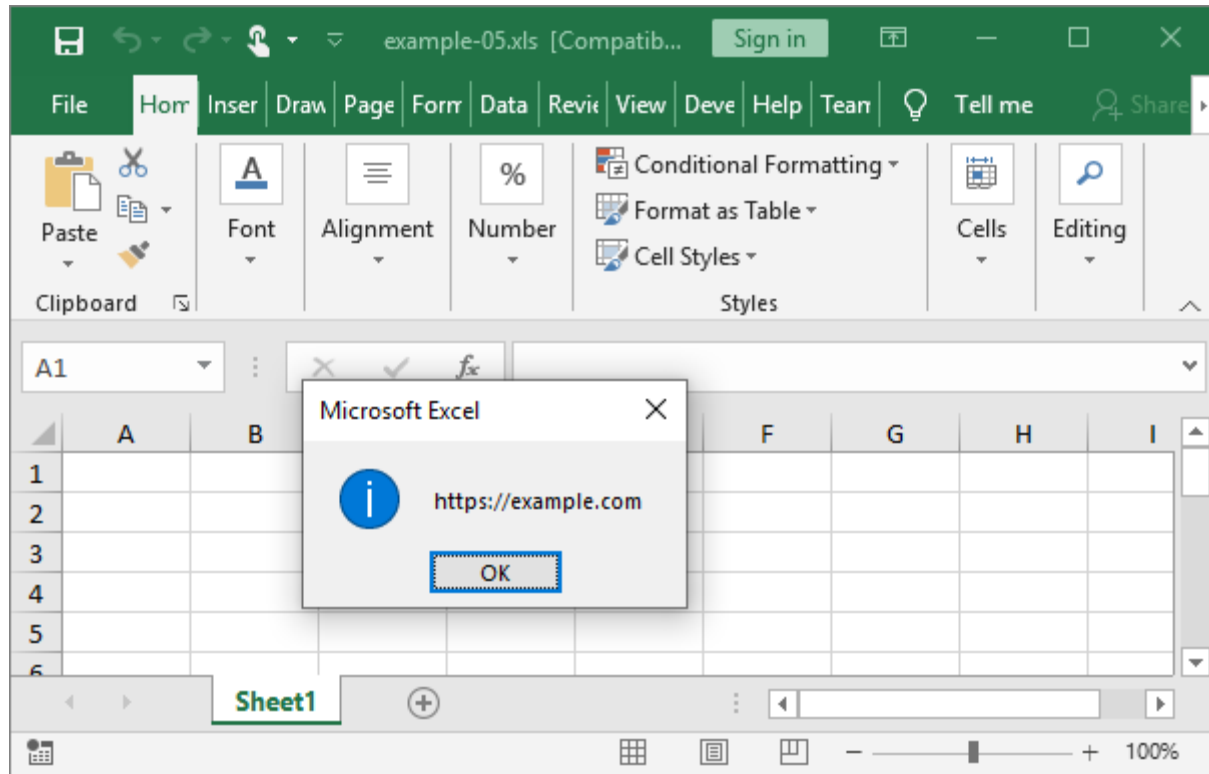
Tip 4: Abuse!



Disclosure

Example 5: unused bits

Tip 4: Abuse!



Example 5: unused bits

Tip 4: Abuse!



```
rule excel_boundsheet_4_macros_ascii_hidden {
  strings:
    $workbook = { 57 00 6F 00 72 00 6B 00 62 00 6F 00 6F 00 6B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 }
    $boundsheetmacro4ascii = { 85 00 ?? 00 ?? ?? ?? ?? 01 01 ?? 00 }
  condition:
    uint32be(0) == 0xd0cf11e0 and
    $workbook and
    $boundsheetmacro4ascii and
    for any i in (1..#boundsheetmacro4ascii): (uint16(@boundsheetmacro4ascii[i] + 2) == uint8(@boundsheetmacro4ascii[i] + 10) + 8)
}

rule excel_boundsheet_4_macros_ascii_very_hidden {
  strings:
    $workbook = { 57 00 6F 00 72 00 6B 00 62 00 6F 00 6F 00 6B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 }
    $boundsheetmacro4ascii = { 85 00 ?? 00 ?? ?? ?? ?? 02 01 ?? 00 }
  condition:
    uint32be(0) == 0xd0cf11e0 and
    $workbook and
    $boundsheetmacro4ascii and
    for any i in (1..#boundsheetmacro4ascii): (uint16(@boundsheetmacro4ascii[i] + 2) == uint8(@boundsheetmacro4ascii[i] + 10) + 8)
}
```


Example 5: unused bits

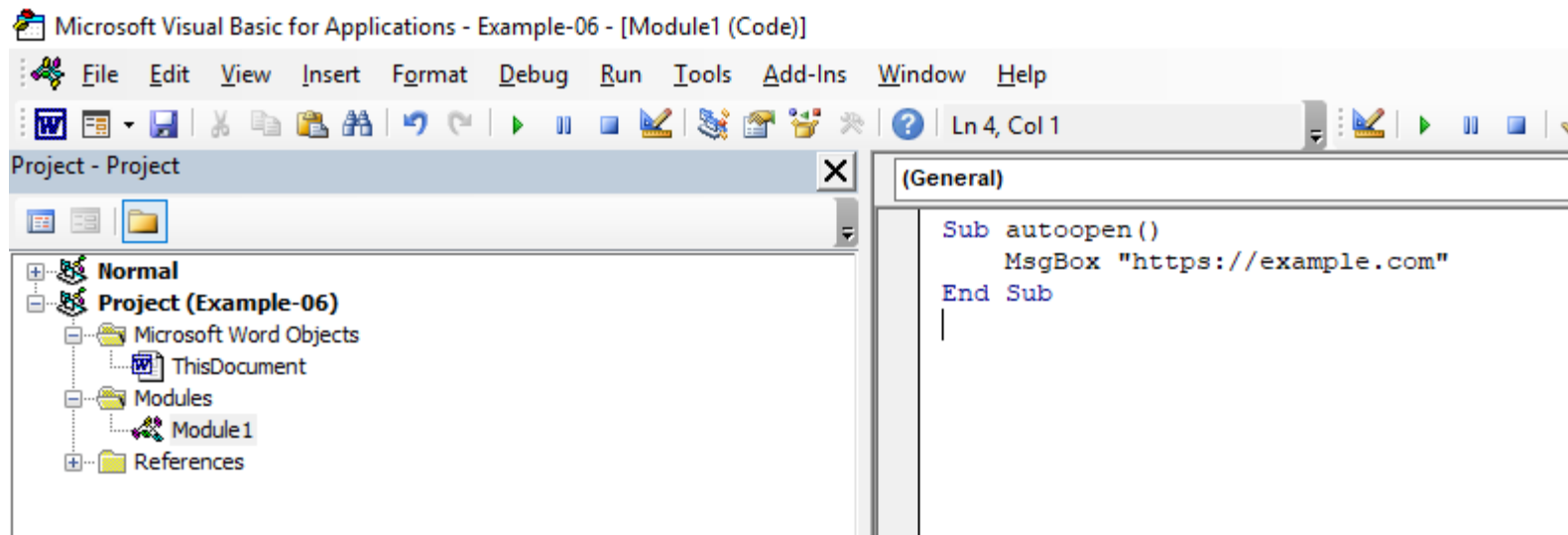
Tip 4: Abuse!



```
rule excel_boundsheet_4_macros_ascii_abnormal_visibility {
  strings:
    $workbook = { 57 00 6F 00 72 00 6B 00 62 00 6F 00 6F 00 6B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 }
    $boundsheetmacro4ascii = { 85 00 ?? 00 ?? ?? ?? ?? ?? 01 ?? 00 }
  condition:
    uint32be(0) == 0xd0cf11e0 and
    $workbook and
    $boundsheetmacro4ascii and
    for any i in (1..#boundsheetmacro4ascii): (uint16(@boundsheetmacro4ascii[i] + 2) == uint8(@boundsheetmacro4ascii[i] + 10) + 8 and
    (uint8(@boundsheetmacro4ascii[i] + 8) > 2))
}
```

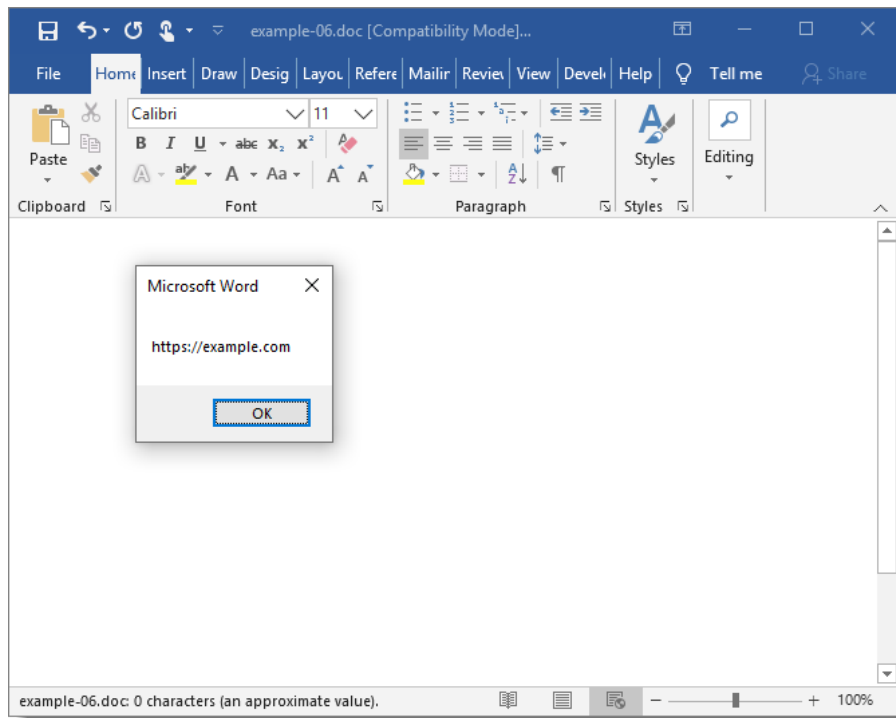
Example 6: VBA stomping

Tip 2: Learn!



Example 6: VBA stomping

Tip 2: Learn!



Example 6: VBA stomping

Tip 2: Learn!

```
@NVISO_Labs C:\Demo>oledump.py -i example-06.doc
1:      114      '\x01CompObj'
2:     4096      '\x05DocumentSummaryInformation'
3:     4096      '\x05SummaryInformation'
4:     7065      '1Table'
5:      415      'Macros/PROJECT'
6:       65      'Macros/PROJECTwm'
7: M   1021    920+101 'Macros/VBA/Module1'
8: m    932    775+157 'Macros/VBA/ThisDocument'
9:     2553      'Macros/VBA/_VBA_PROJECT'
10:      569      'Macros/VBA/dir'
11:     4096      'WordDocument'

@NVISO_Labs C:\Demo>
```

Example 6: VBA stomping

Tip 2: Learn!

2.3.4.3 Module Stream: Visual Basic Modules

Specifies the source code for a **module**.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
PerformanceCache (variable)																															
...																															
CompressedSourceCode (variable)																															
...																															

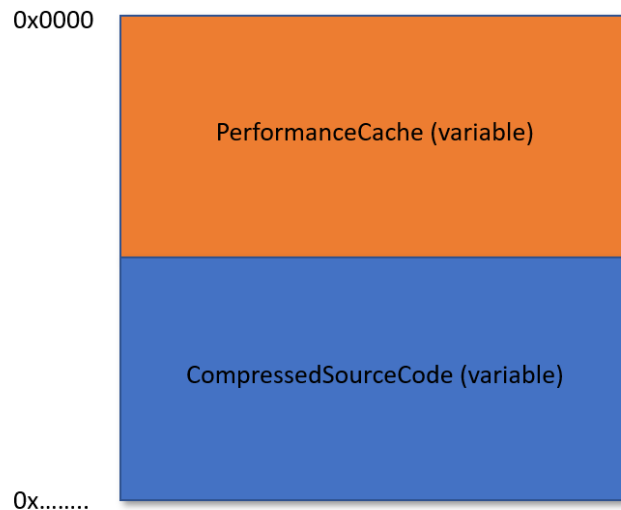
PerformanceCache (variable): An array of bytes that forms an implementation-specific and version-dependent performance cache for the module. MUST be **MODULEOFFSET** (section 2.3.4.2.3.2.5) bytes in size. MUST be ignored on read.

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).

Example 6: VBA stomping

Tip 2: Learn!

Module Stream:



Example 6: VBA stomping

Tip 2: Learn!



```
@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 .....EA.s...
00000030: FF 03 00 00 00 00 00 00 00 B6 00 FF FF 01 01 00 .....
00000040: 00 00 00 FF FF FF FF 00 00 00 FF FF 04 00 FF .....
00000050: FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000080: 00 00 00 00 00 00 00 10 00 00 03 00 00 00 05 .....
00000090: 00 00 00 07 00 00 00 FF FF FF FF FF FF FF 01 .....
000000A0: 01 08 00 00 00 FF FF FF FF 78 00 00 00 02 00 00 .....X.....
000000B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000C0: 00 00 00 00 00 00 00 00 00 00 00 00 FF FF .....
000000D0: 00 00 00 00 4D 45 00 00 FF FF FF FF FF FF 00 00 ....ME.....
000000E0: 00 00 FF FF 00 00 00 00 FF FF 01 01 00 00 00 00 .....
000000F0: DF 00 FF FF 00 00 00 00 04 00 FF FF FF FF FF FF .....
00000100: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000110: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000120: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000130: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000140: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000150: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000160: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
00000170: FF FF FF FF FF FF FF FF FF FF 28 00 00 00 00 00 .....(.....
00000180: 36 0A FF FF FF FF 00 00 00 00 02 3C 08 00 FF FF 6.....<.....
00000190: 00 00 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 .....
```

Example 6: VBA stomping

Tip 2: Learn!



```
@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 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
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>
```


Example 6: VBA stomping

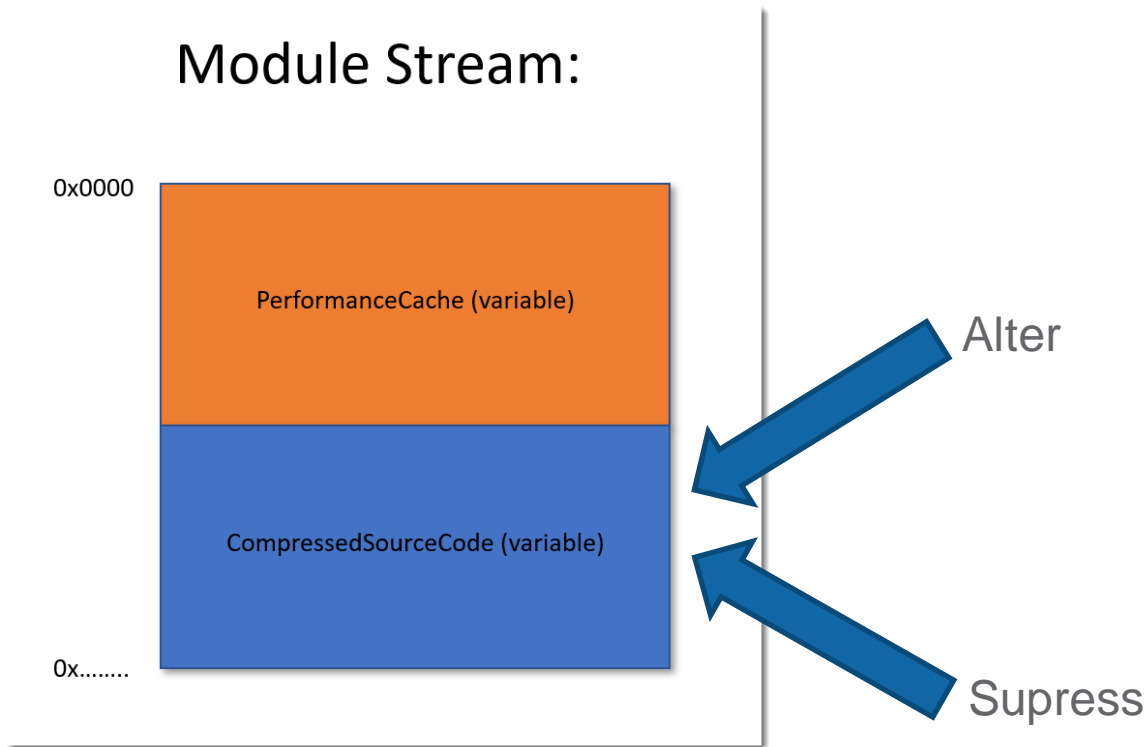
Tip 2: Learn!

```
@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>
```

Example 6: VBA stomping

Tip 2: Learn!



Example 6: VBA stomping

Tip 2: Learn!

```
@Nviso_Labs C:\Demo>oledump.py -i example-06b.doc

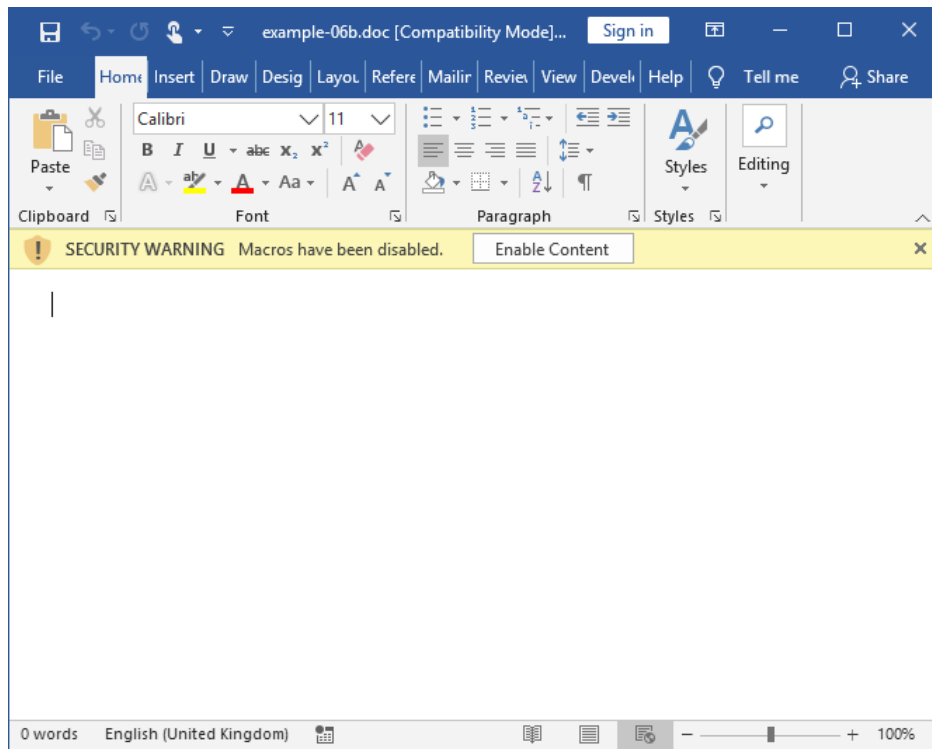
1:      114      '\x01CompObj'
2:     4096      '\x05DocumentSummaryInformation'
3:     4096      '\x05SummaryInformation'
4:     7065      '1Table'
5:      415      'Macros/PROJECT'
6:       65      'Macros/PROJECTwm'
7: m    957      920+37 'Macros/VBA/Module1'
8: m    932      775+157 'Macros/VBA/ThisDocument'
9:     2553      'Macros/VBA/_VBA_PROJECT'
10:      569      'Macros/VBA/dir'
11:     4096      'WordDocument'

@Nviso_Labs C:\Demo>oledump.py -s 7 -v example-06b.doc
Attribute VB_Name = "Module1"

@Nviso_Labs C:\Demo>
```

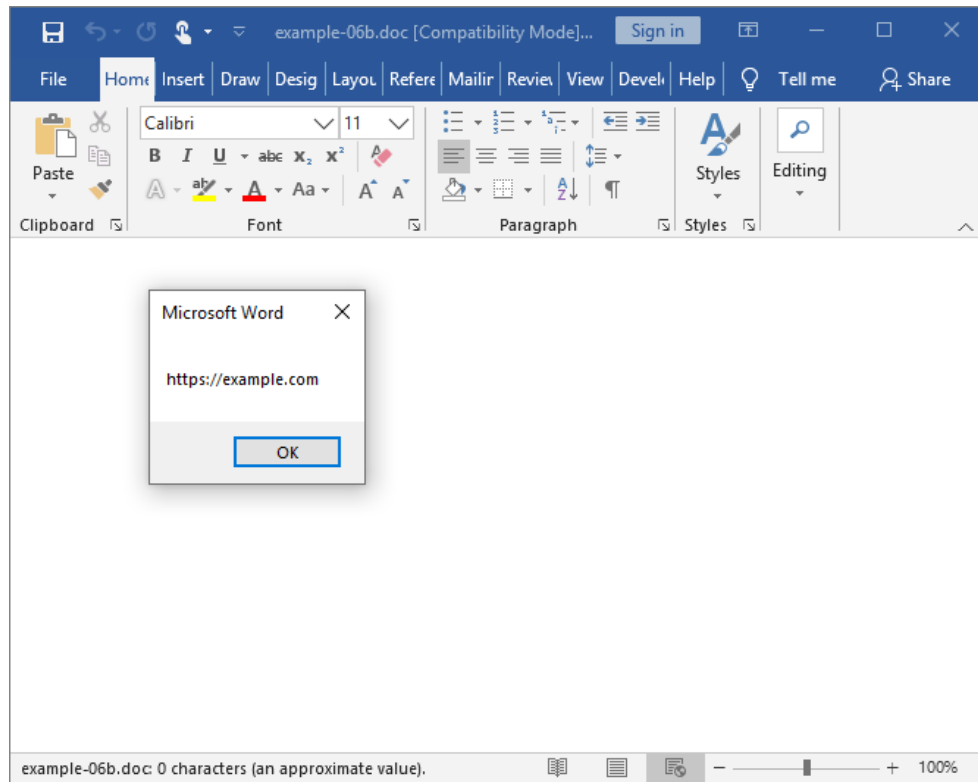
Example 6: VBA stomping

Tip 2: Learn!



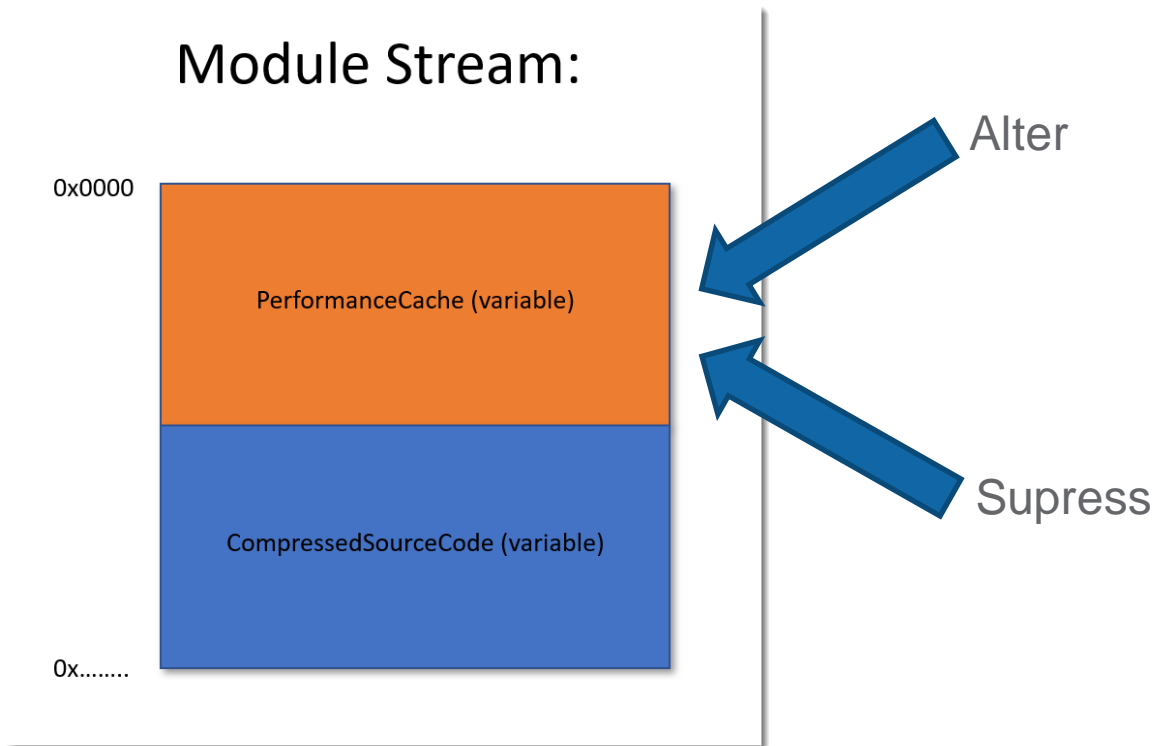
Example 6: VBA stomping

Tip 2: Learn!



Example 7: VBA purging

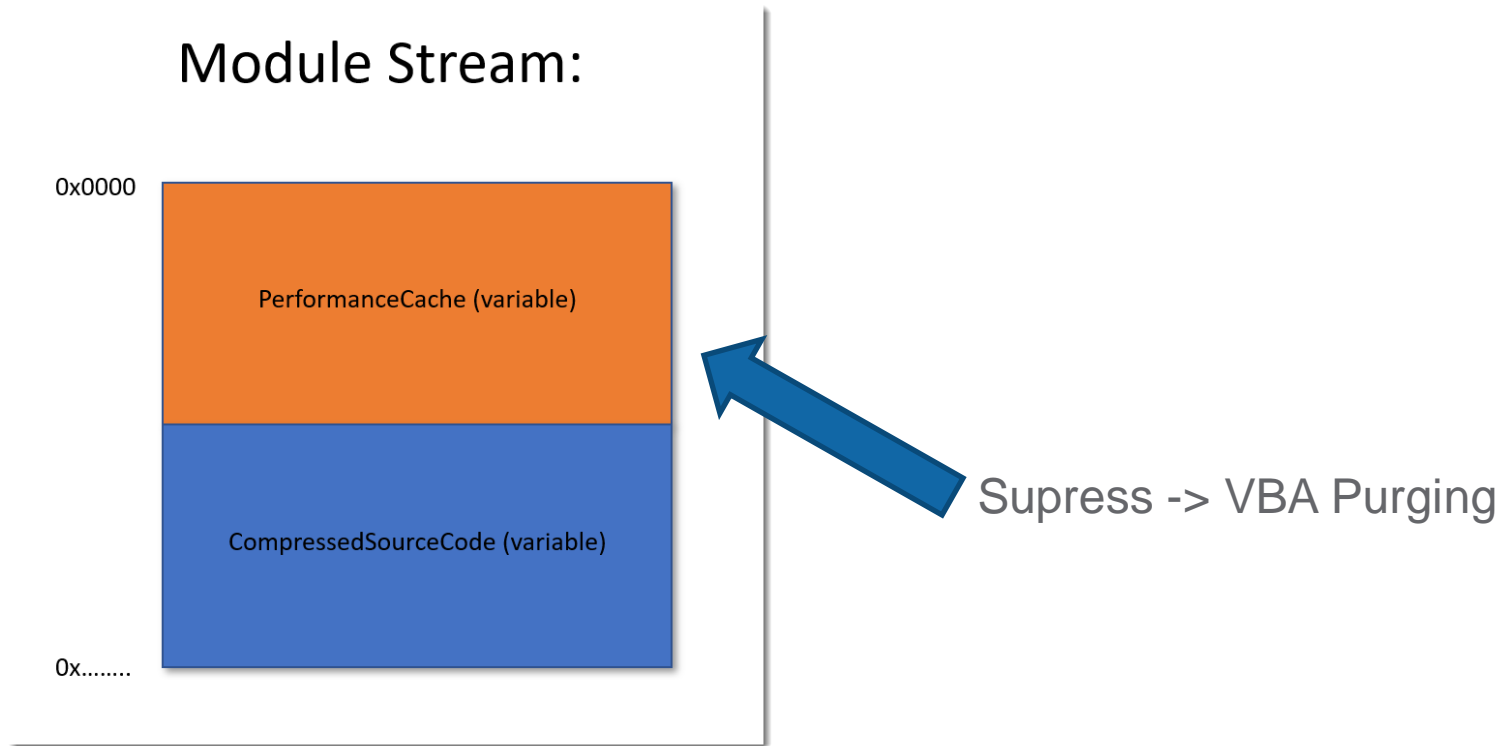
Tip 3: Use!



Example 7: VBA purging

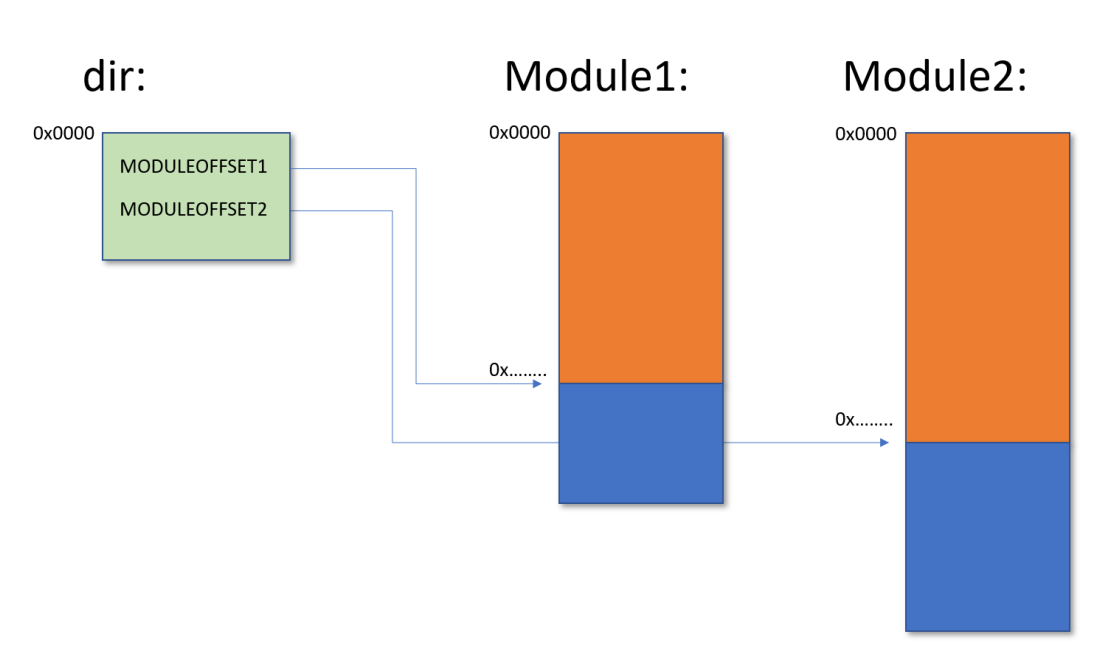
Tip 3: Use!

Module Stream:



Example 7: VBA purging

Tip 3: Use!



Example 7: VBA purging

Tip 3: Use!

C:\ @NVISO_Labs

```
@NVISO_Labs C:\Demo>oledump.py -i example-07.doc
```

```
1:      114      '\x01CompObj'  
2:     4096      '\x05DocumentSummaryInformation'  
3:     4096      '\x05SummaryInformation'  
4:     7065      '1Table'  
5:      415      'Macros/PROJECT'  
6:       65      'Macros/PROJECTwm'  
7: M      101      0+101 'Macros/VBA/Module1'  
8: m      157      0+157 'Macros/VBA/ThisDocument'  
9:        7      'Macros/VBA/_VBA_PROJECT'  
10:     534      'Macros/VBA/dir'  
11:     4096      'WordDocument'
```

```
@NVISO_Labs C:\Demo>
```

Example 7: VBA purging

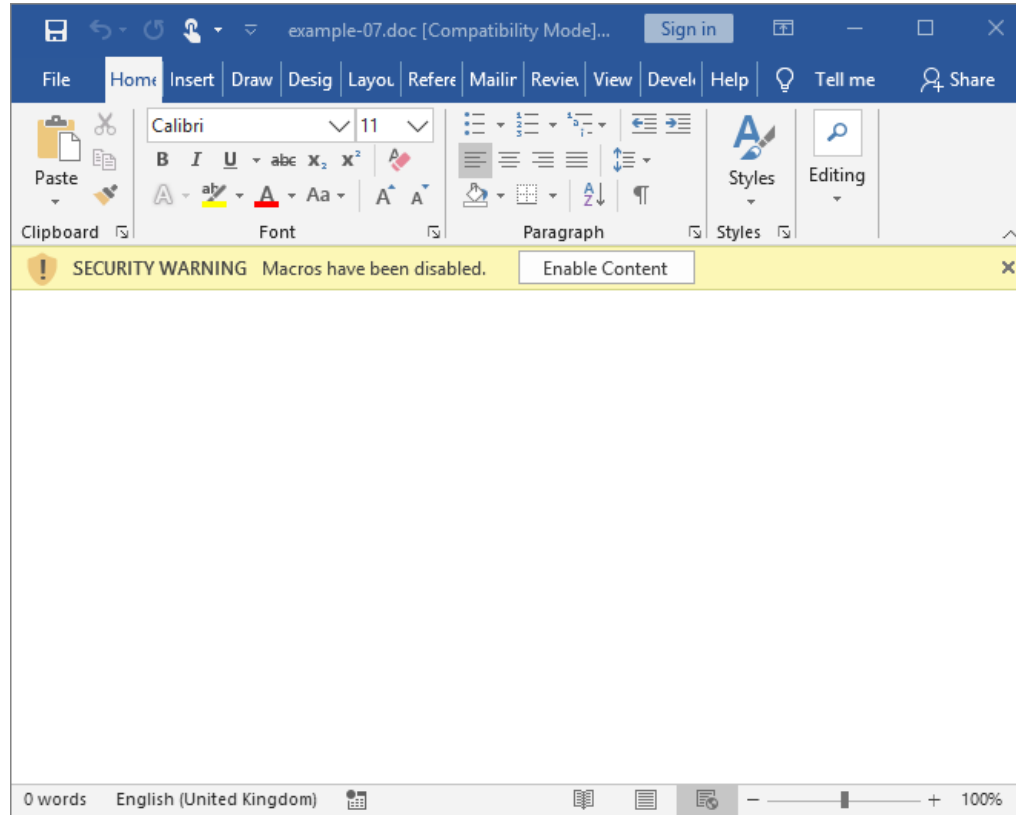
Tip 3: Use!

```
@NISO_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
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..

@NISO_Labs C:\Demo>
```

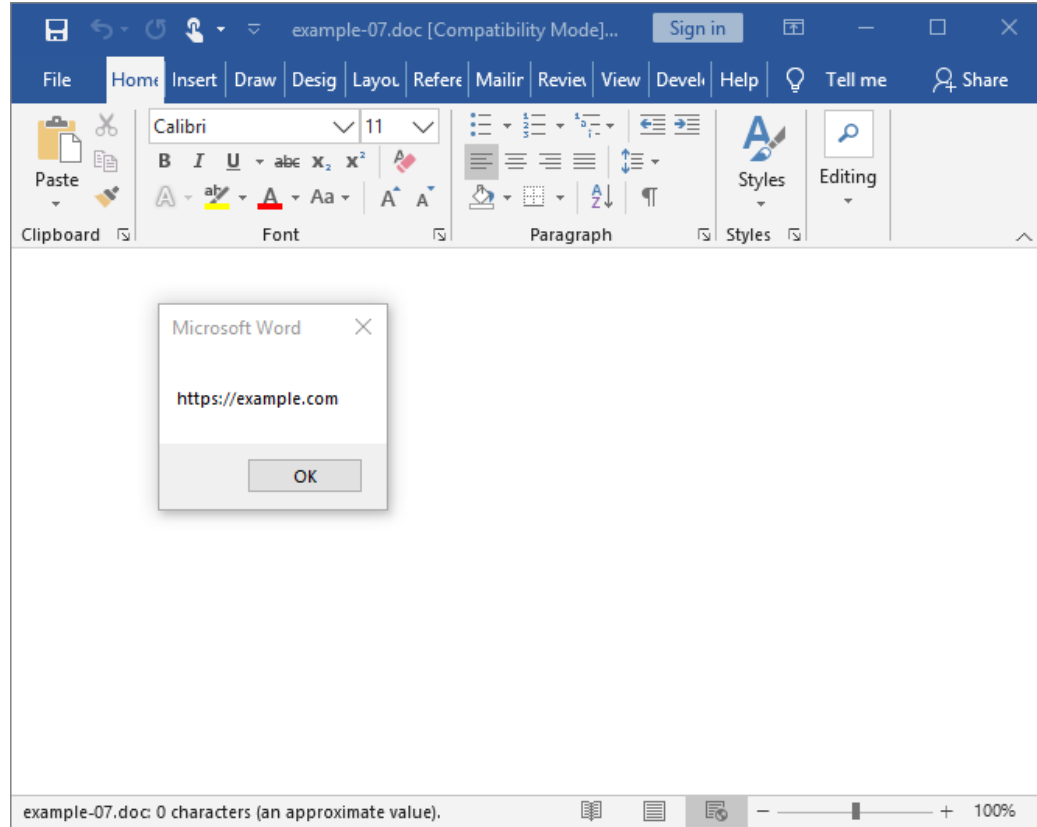
Example 7: VBA purging

Tip 3: Use!



Example 7: VBA purging

Tip 3: Use!



Example 7: VBA purging

Tip 3: Use!



44
/ 61

Community Score

44 engines detected this file

b829ef640b3ee2965e25453727598509aff4a461d41ac7d1be56d8c8f917c2c1

Tracking-42398631-BUD-HWN.doc

create-ole

doc

macros

obfuscated

run-file

176.00 KB

Size

2019-12-27 11:17:41 UTC

6 hours ago

DOC

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 3

Ad-Aware	W97M.Downloader.GRU	AegisLab	Trojan.MSWord.Agent.alc
ALYac	Trojan.Downloader.VBA.gen	Antiy-AVL	Trojan[Downloader]MSOffice.Agent.hic
Arcabit	HEUR.VBA.Trojan.e	Avast	VBA.Downloader-GCD [Trj]
AVG	VBA.Downloader-GCD [Trj]	Avira (no cloud)	W97M/Agent.36885547
Baidu	VBA.Trojan-Downloader.Agent.cpw	BitDefender	W97M.Downloader.GRU

Example 7: VBA purging

Tip 3: Use!



15
/ 60

Community Score

15 engines detected this file

e7788fbbf072b34484abe68255a63b8722f0dd406d3f2f68ce956bd92e60e3b6
b829ef640b3ee2965e25453727598509aff4a461d41ac7d1be56d8c8f917c2c1-no-source-code.vir

doc

143.00 KB
Size

2019-12-22 13:29:25 UTC
5 days ago

DOC

DETECTION

DETAILS

BEHAVIOR

COMMUNITY

Ad-Aware	1 VBA.Maldade.8.Gen	Arcabit	1 VBA.Maldade.8.Gen
Avira (no cloud)	1 W97M/Agent.36885547	BitDefender	1 VBA.Maldade.8.Gen
Cyren	1 W97M/Agent	Emsisoft	1 VBA.Maldade.8.Gen (B)
eScan	1 VBA.Maldade.8.Gen	F-Prot	1 New Or Modified W97M/Agent
F-Secure	1 Malware.W97M/Agent.36885547	FireEye	1 VBA.Maldade.8.Gen
GData	1 VBA.Maldade.8.Gen	Ikarus	1 Trojan-Downloader.VBA.Agent
MAX	1 Malware (ai Score=80)	TrendMicro	1 W2KM_EMOTET.TICBOAH
TrendMicro-HouseCall	1 W2KM_EMOTET.TICBOAH	AegisLab	1 Undetected
AhnLab-V3	1 Undetected	ALYac	1 Undetected

Example 7: VBA purging

Tip 3: Use!



16
/ 58

Community Score

16 engines detected this file

f44e067e011ab13bddf3e3143ea427090ac07c59dcb434d069bcefb4fe3cb434b829ef640b3ee2965e25453727598509aff4a461d41ac7d1be56d8c8f917c2c1-no-p-code.vir

76.00 KB
Size

2019-12-22 13:29:56 UTC
5 days ago

DOC

create-ole

doc

macros

obfuscated

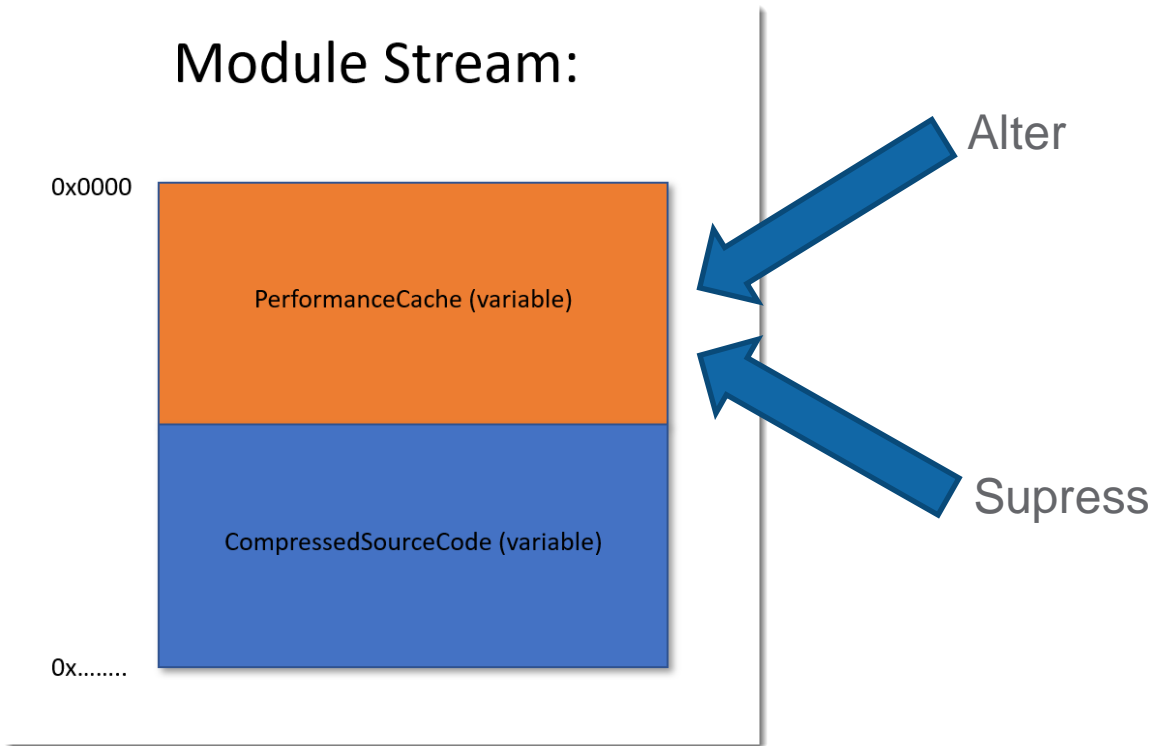
run-file

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY 1
Antiy-AVL	1 Trojan[Downloader]MSOffice.Agent.hic	Arcabit	1 HEUR.VBA Trojan.e	
Avast	1 VBA:Downloader-GCD [Trj]	AVG	1 VBA:Downloader-GCD [Trj]	
Baidu	1 VBA.Trojan-Downloader.Agent.cpw	Endgame	1 Malicious (high Confidence)	
ESET-NOD32	1 VBA/TrojanDownloader.Agent.HIC	Fortinet	1 VBA/Agent.HHV/tr	
Ikarus	1 Trojan-Downloader.VBA.Agent	McAfee-GW-Edition	1 BehavesLike.Downloader.Ig	
Rising	1 Macro.Run.d (CLASSIC)	Sangfor Engine Zero	1 Malware	
SentinelOne (Static ML)	1 DFI - Malicious OLE	Sophos AV	1 Troj/DocDI-NCG	
TACHYON	1 Trojan/W97M.Agent.Gen	Tencent	1 Heur:Trojan.Script.LS_Gencirc.7071761.0	
BitDam ATP	1 MALWARE	Ad-Aware	Undetected	
AegisLab	Undetected	AhnLab-V3	Undetected	

Example 8: Code signing tampering

Tip 4: Abuse!

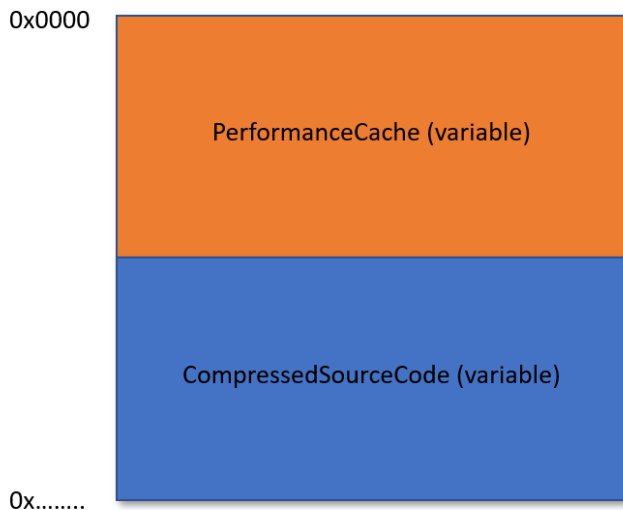
Module Stream:



Example 8: Code signing tampering

Tip 4: Abuse!

Module Stream:



Alter -> code signing tampering

Disclosure

Example 8: Code signing tampering

Tip 4: Abuse!



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.

Example 8: Code signing tampering

Tip 4: Abuse!



```
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
```

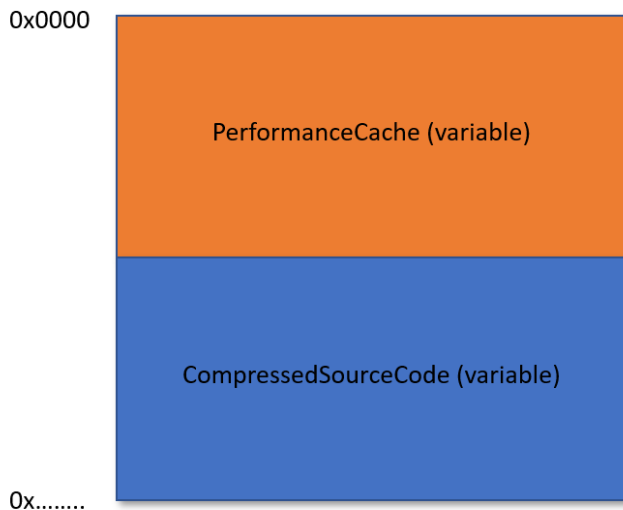
72 / 111

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

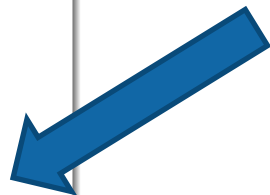
Example 8: Code signing tampering

Tip 4: Abuse!

Module Stream:

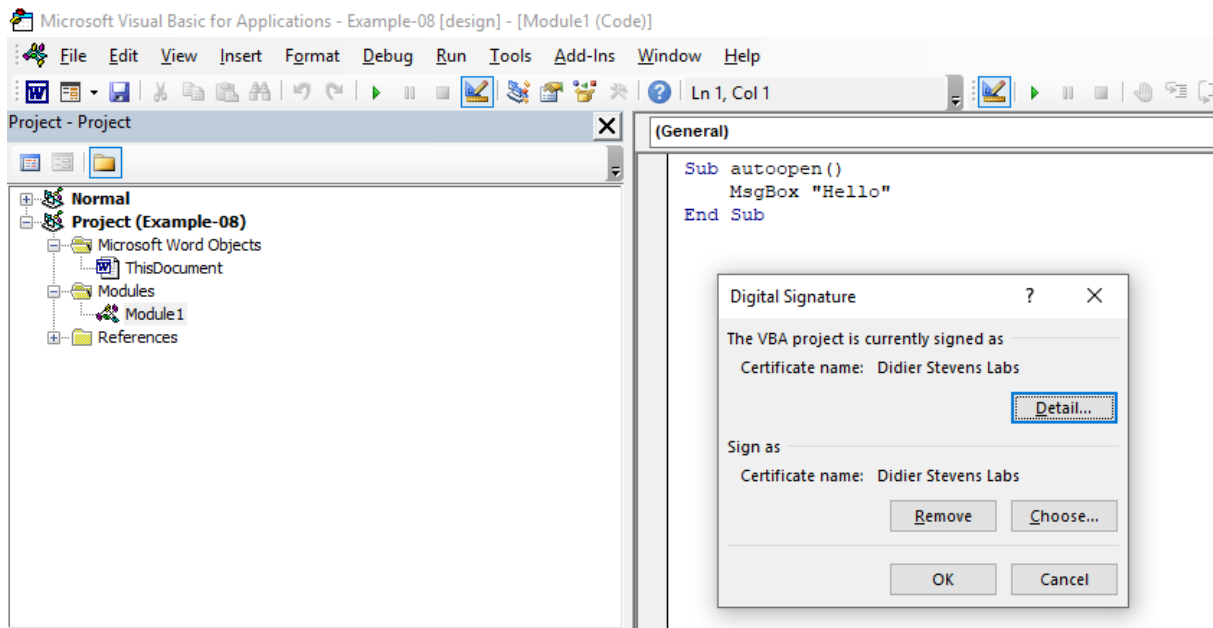


Ignored for contents hashes



Example 8: Code signing tampering

Tip 4: Abuse!



Example 8: Code signing tampering

Tip 4: Abuse!



```
C:\@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>
```

Example 8: Code signing tampering

Tip 4: Abuse!



```
C:\> @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>
```

Example 8: Code signing tampering

Tip 4: Abuse!



```
C:\ @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>
```


Example 8: Code signing tampering

Tip 4: Abuse!



@NVISIO_Labs

```
@NVISIO_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
```

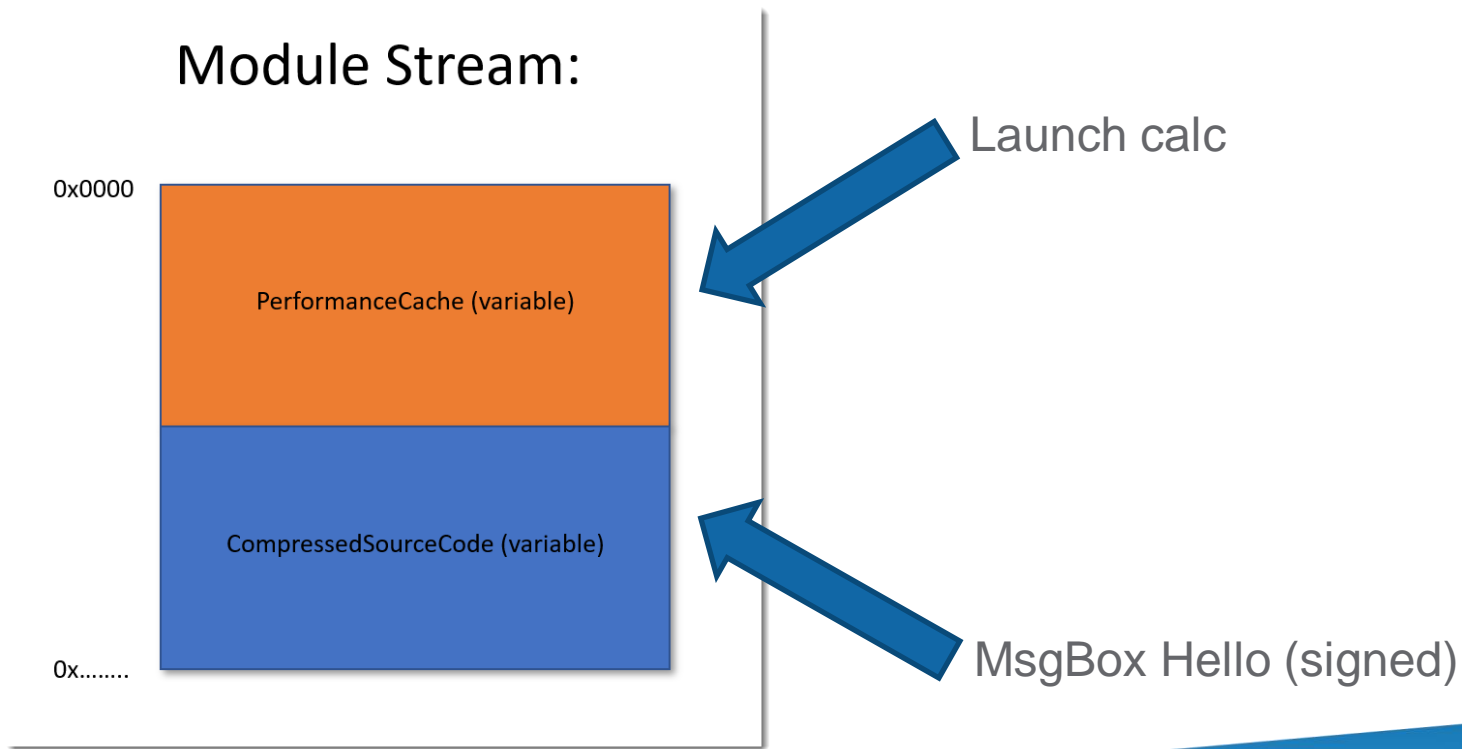
```
Line #2:
```

```
    EndSub
```

```
@NVISIO_Labs C:\Demo>
```

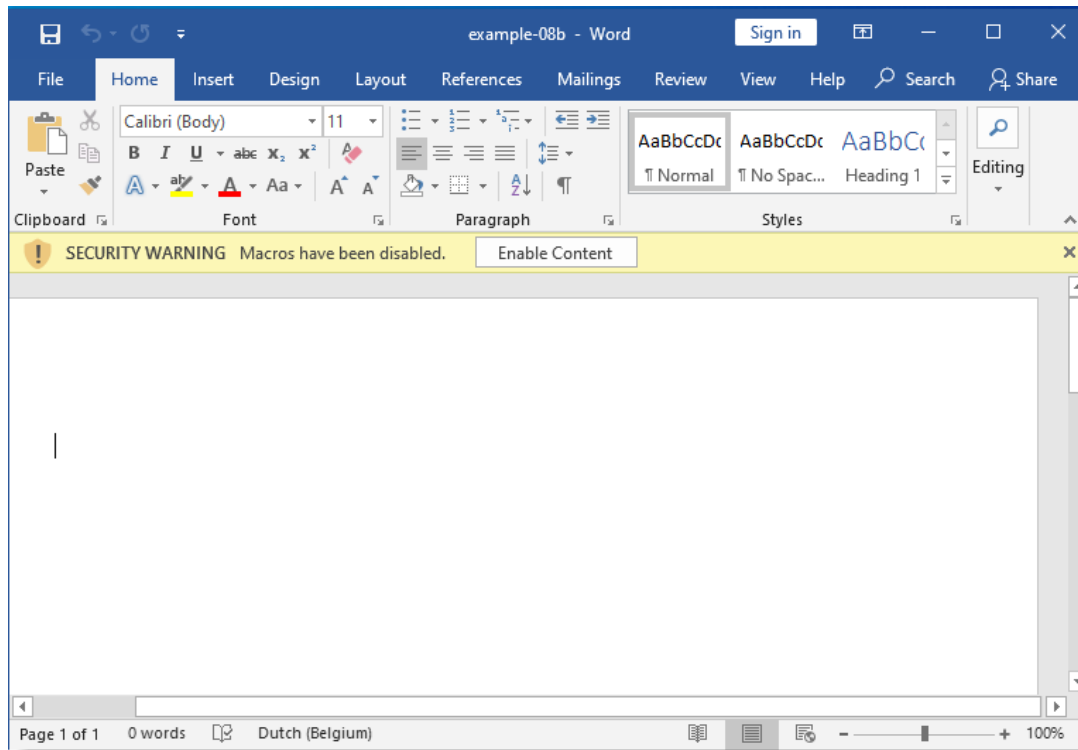
Example 8: Code signing tampering

Tip 4: Abuse!



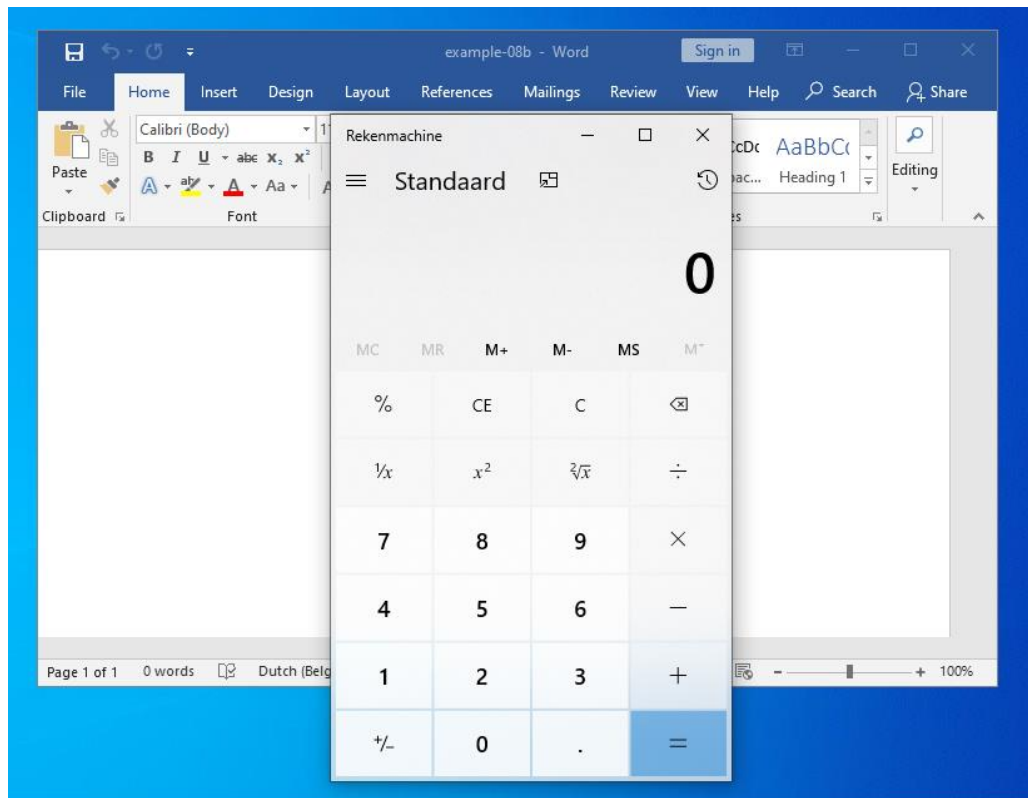
Example 8: Code signing tampering

Tip 4: Abuse!



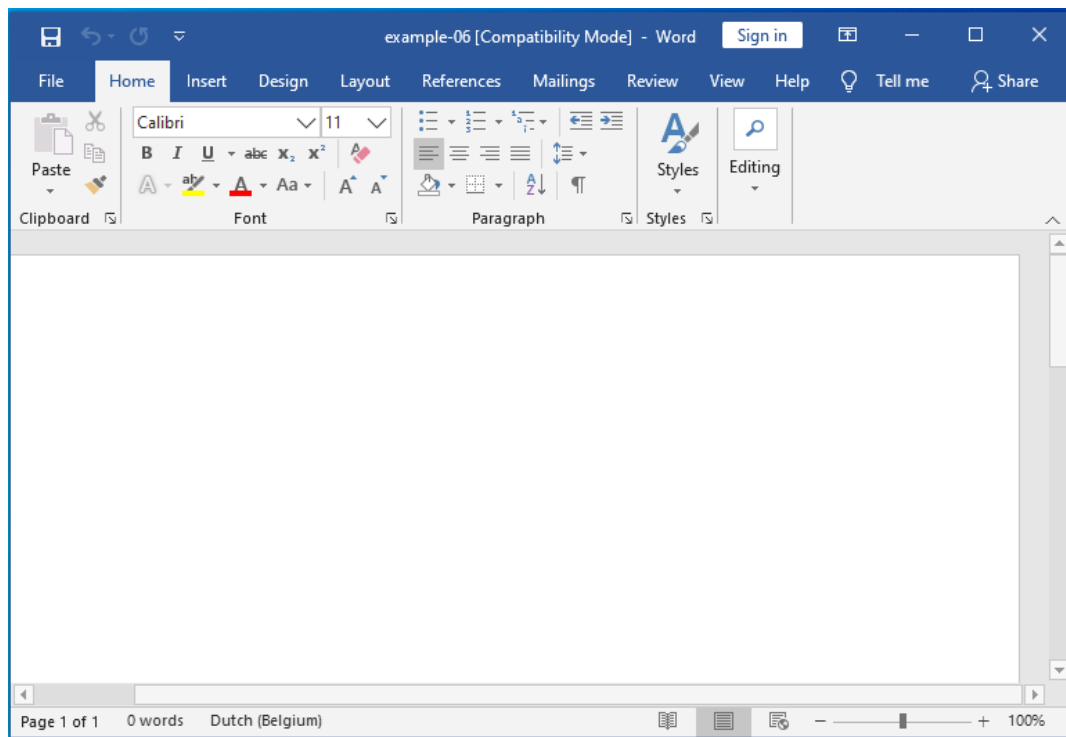
Example 8: Code signing tampering

Tip 4: Abuse!



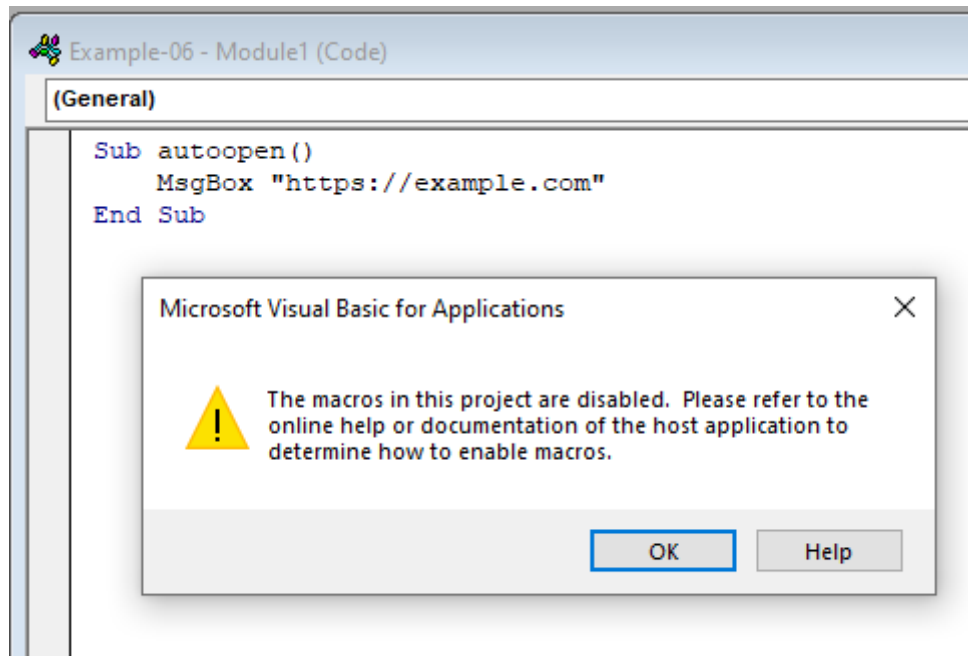
Example 8: Code signing tampering

Tip 4: Abuse!



Example 8: Code signing tampering

Tip 4: Abuse!



Overview examples

1 The power of strings

2 Limiting the power of strings

3 Very hidden

4 Very, very hidden? (D)

5 Unused bits (D)

6 VBA stomping

7 VBA purging

8 Code signing tampering (D)

4 tips for red teamers

1 Analyze your `sh+chr(105)+t`

2 Learn from actors

3 RTFM & use it

4 RTFM & abuse it

More info

<https://isc.sans.edu>

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

<https://blog.nviso.eu>

<https://blog.didierstevens.com>

www.nviso.eu



Questions?

Thank you

www.nviso.eu

