www.nviso.eu

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

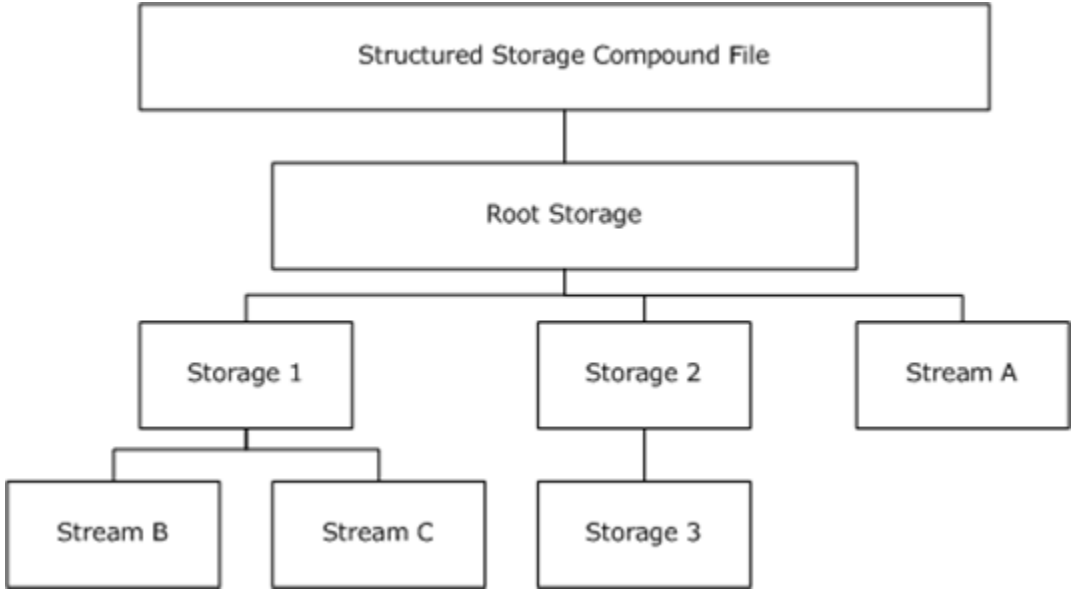
ZIP + XMLs (+ sometimes a bit more)

.docx, .docm, .xlsx, …

CFBF: Compound File Binary Format

I like to call this OLE format

.doc, .xls, …


Structured Storage Compound File
Root Storage
Storage 1
Storage 2
Stream A
Stream B
Stream C
Storage 3

4 tips for red teamers

www.nviso.eu

4 tips for red teamers

1 Analyze your sh+chr(105)+t

nviso

4 tips for red teamers

1. Analyze your sh+chr(105)+t
2. Learn from actors

nviso

4 tips for red teamers

1. Analyze your sh+chr(105)+t
2. Learn from actors
3. RTFM & use it

nviso

4 tips for red teamers

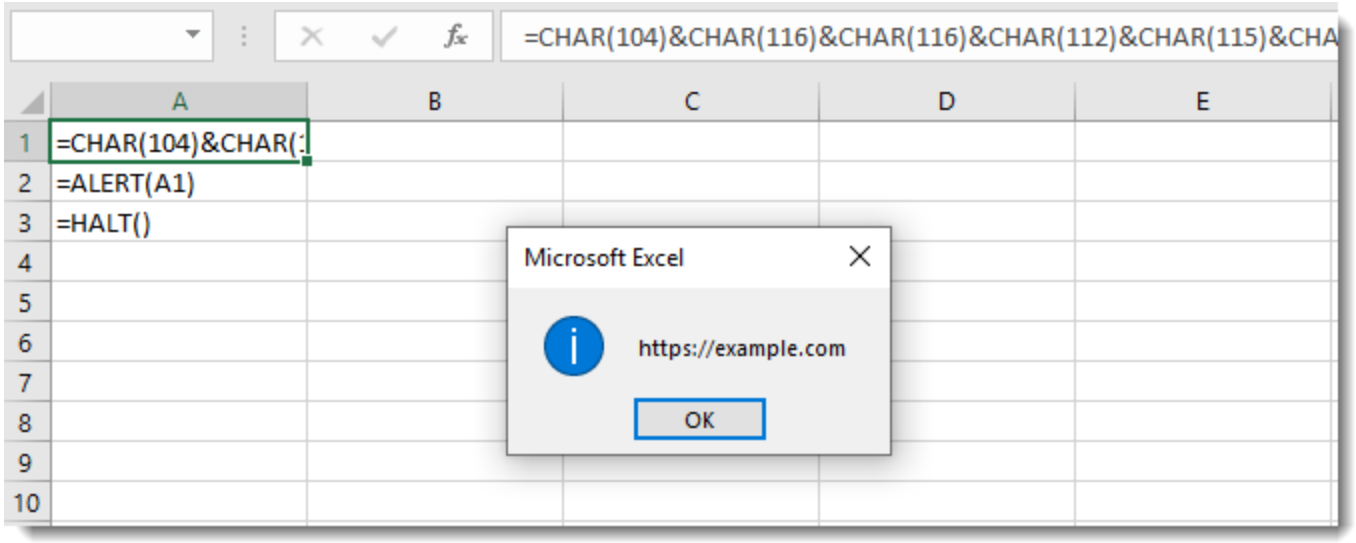
1. Analyze your sh+chr(105)+t
2. Learn from actors
3. RTFM & use it
4. RTFM & abuse it

nviso

Examples (with some disclosures)

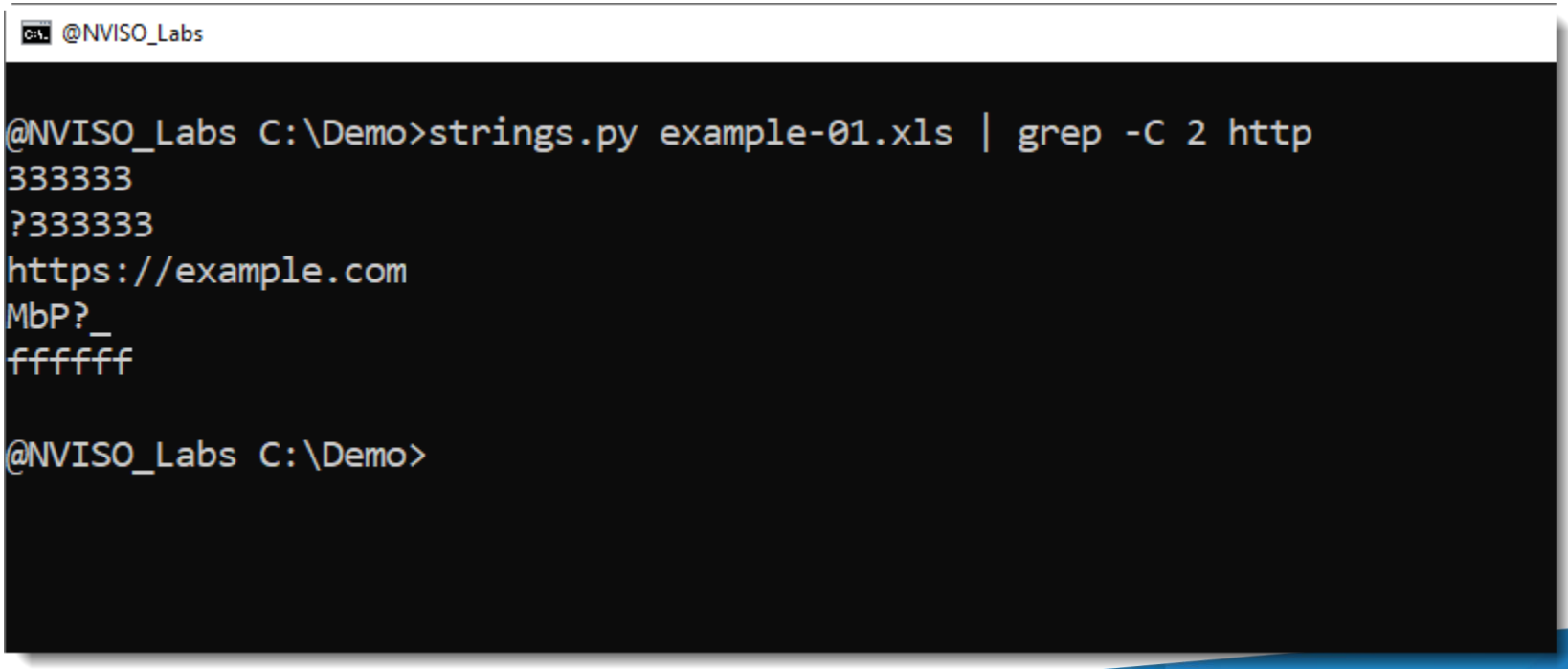
Example 1: the power of strings

Tip 1: Analyze!



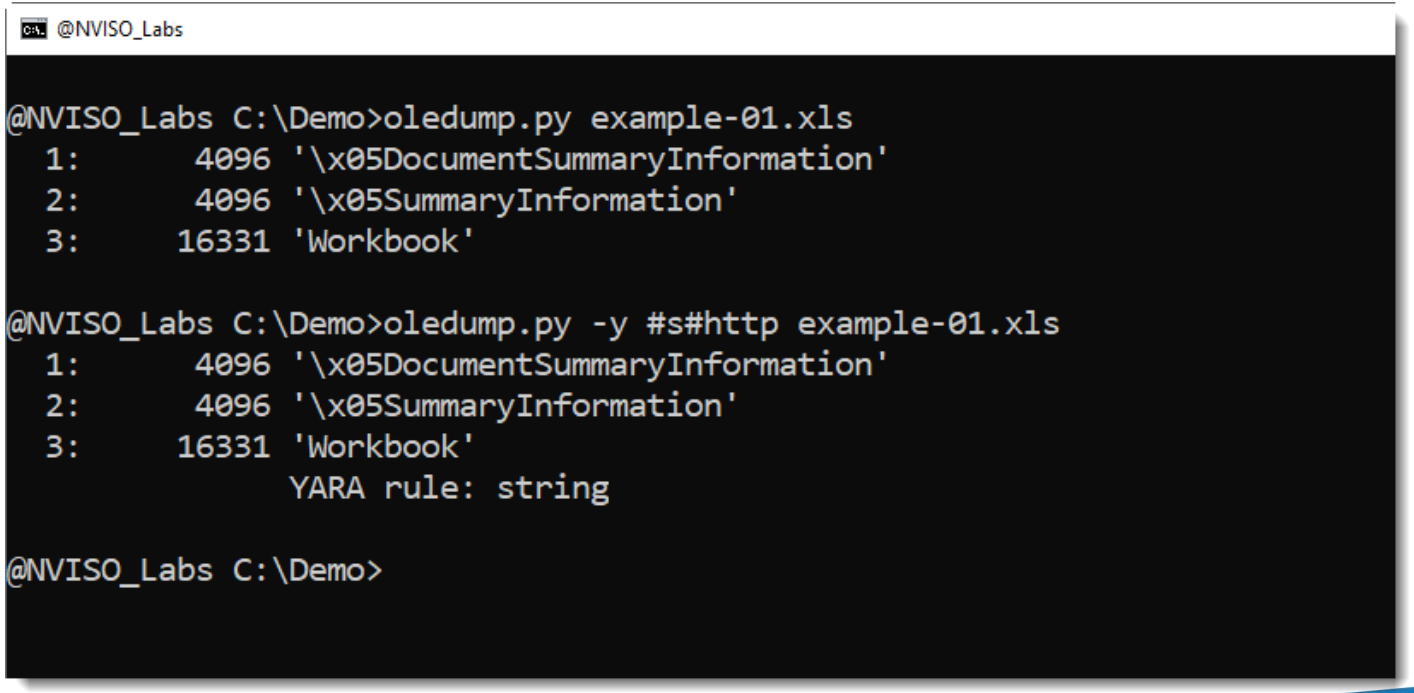
Example 1: the power of strings

Tip 1: Analyze!



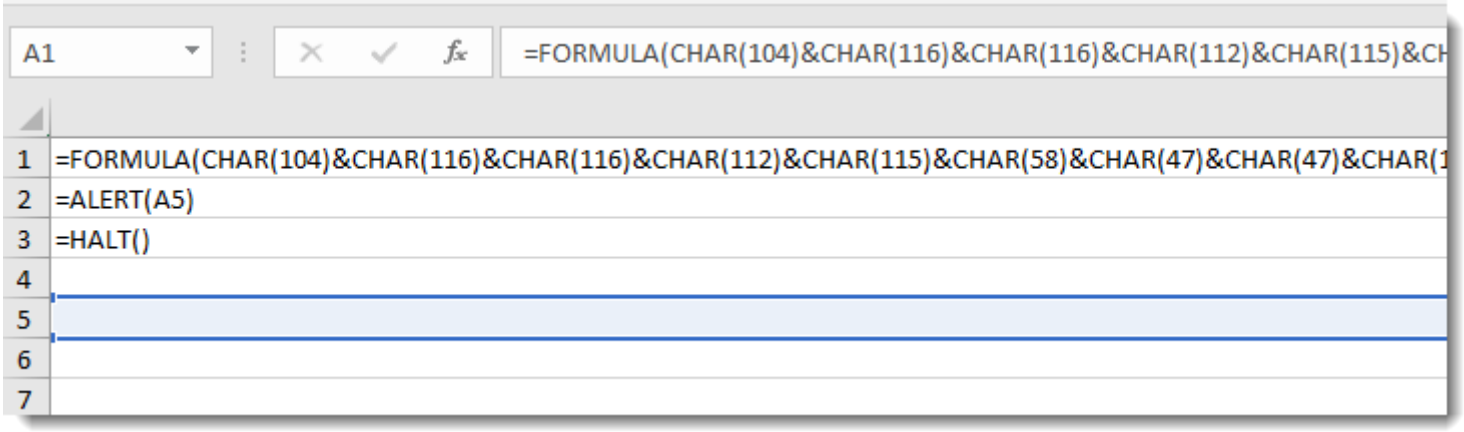
Example 1: the power of strings

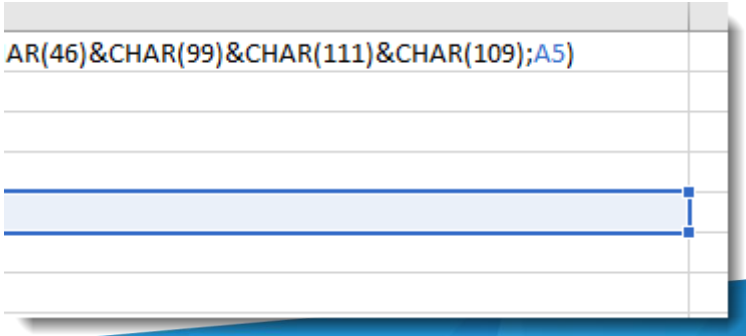
Tip 1: Analyze!



Example 2: limiting the power of strings

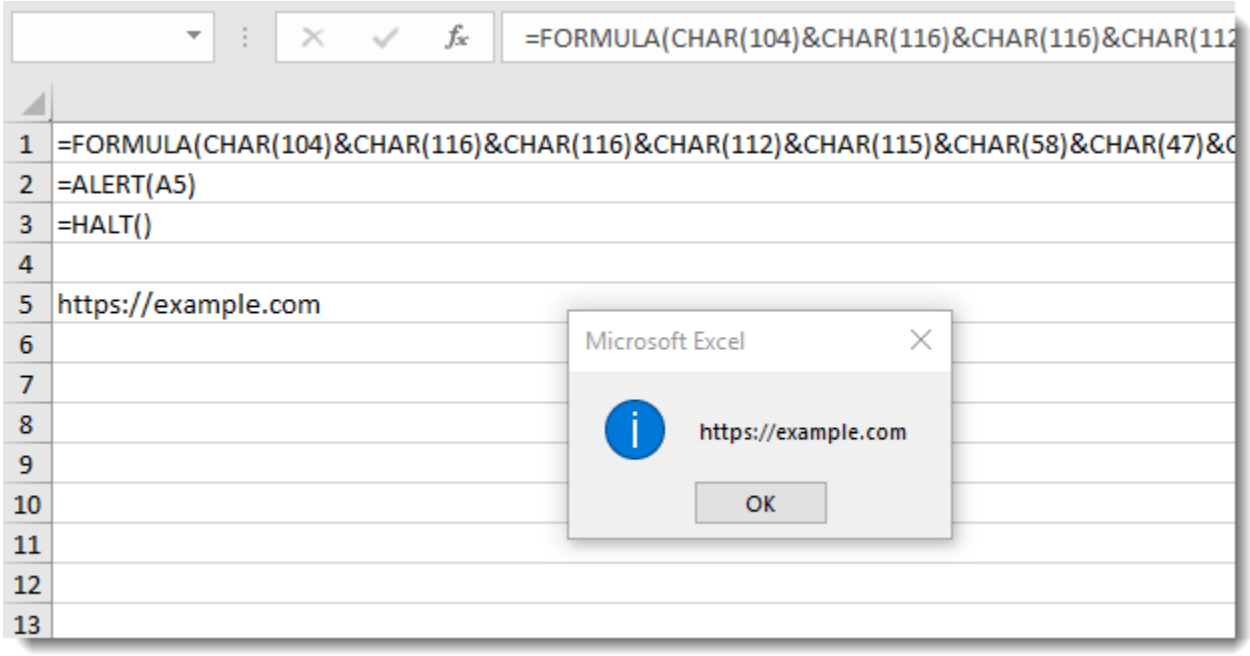
Tip 2: Learn!





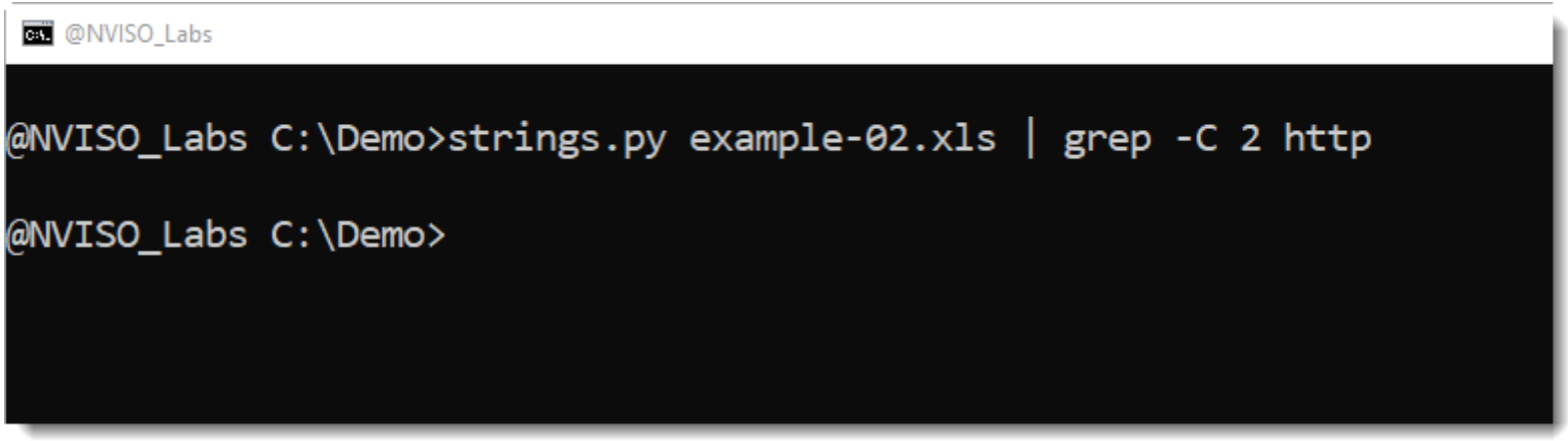
Example 2: limiting the power of strings

Tip 2: Learn!



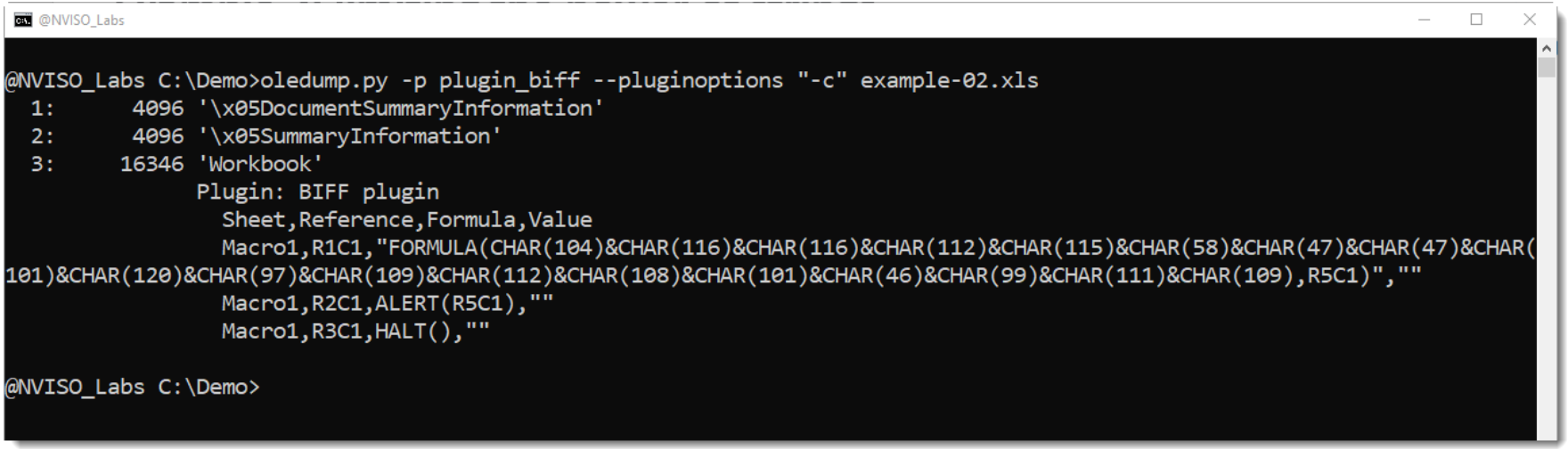
Example 2: limiting the power of strings

Tip 2: Learn!



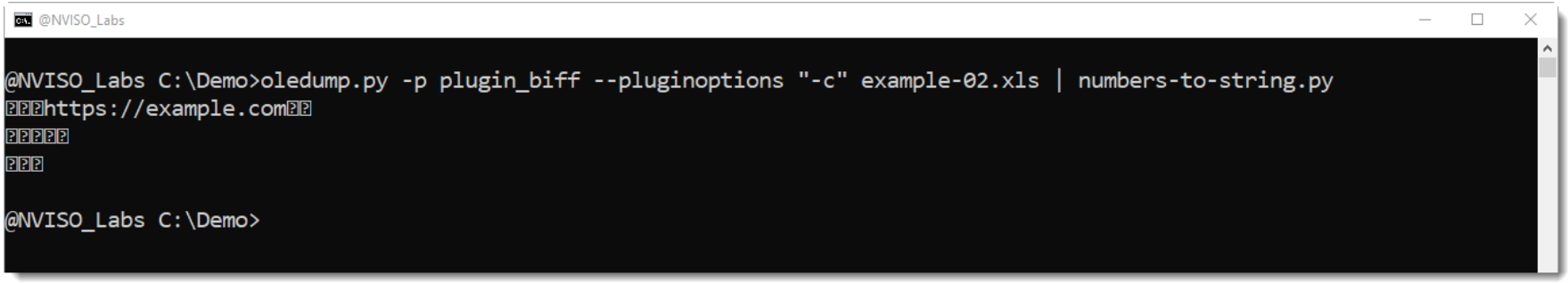
Example 2: limiting the power of strings

Tip 2: Learn!



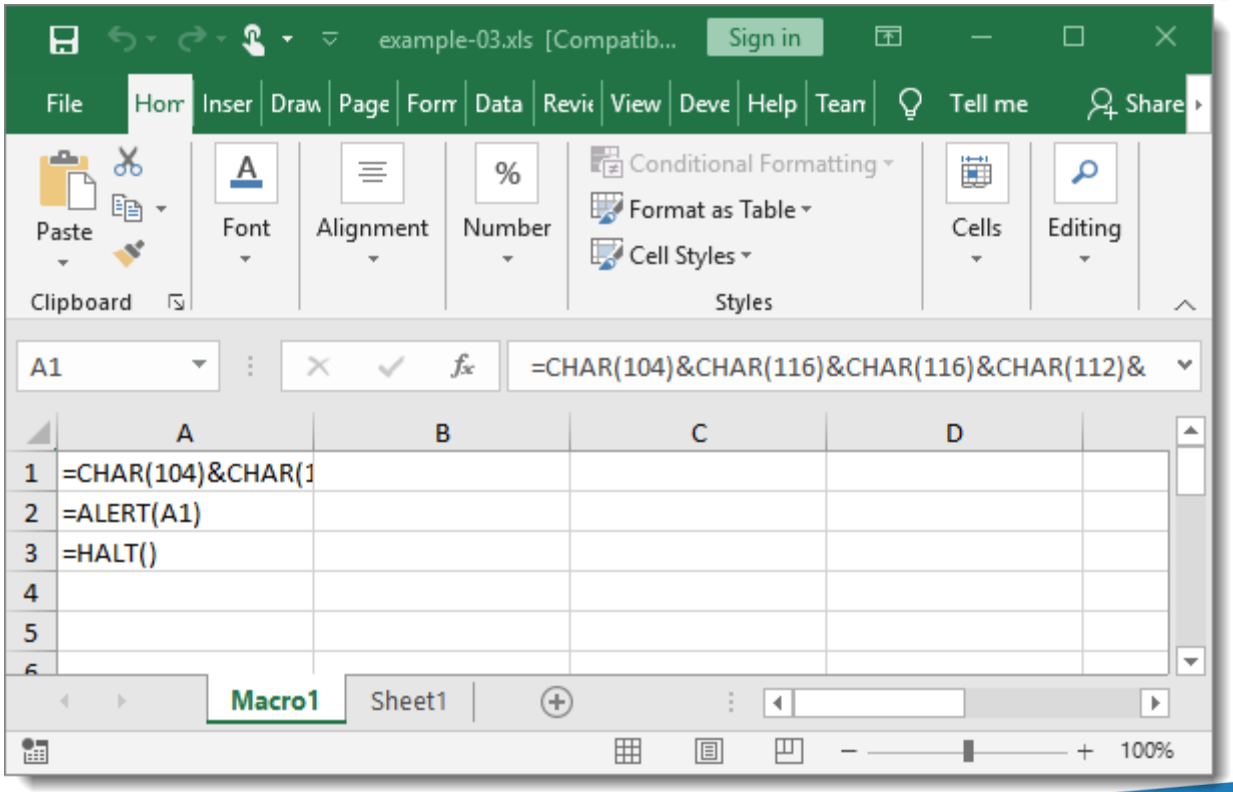
Example 2: limiting the power of strings

Tip 2: Learn!



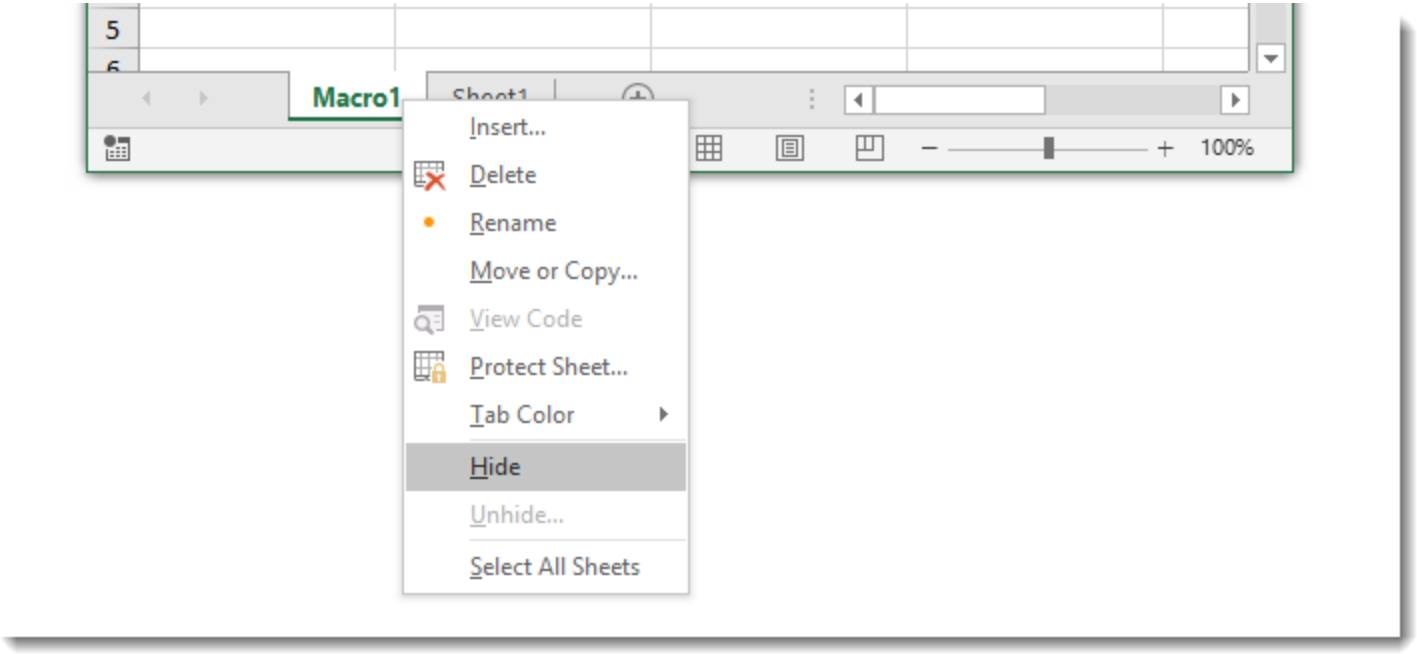
Example 3: very hidden

Tip 3: Use!



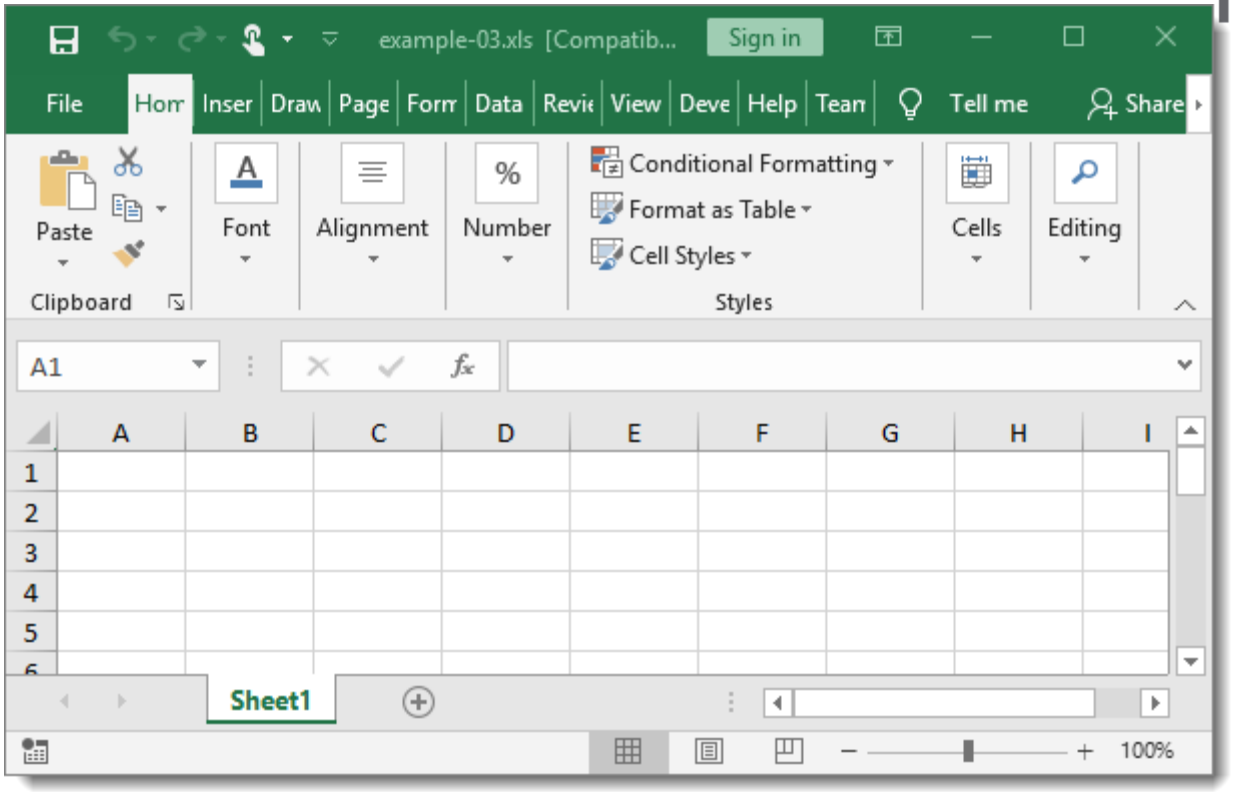
Example 3: very hidden

Tip 3: Use!



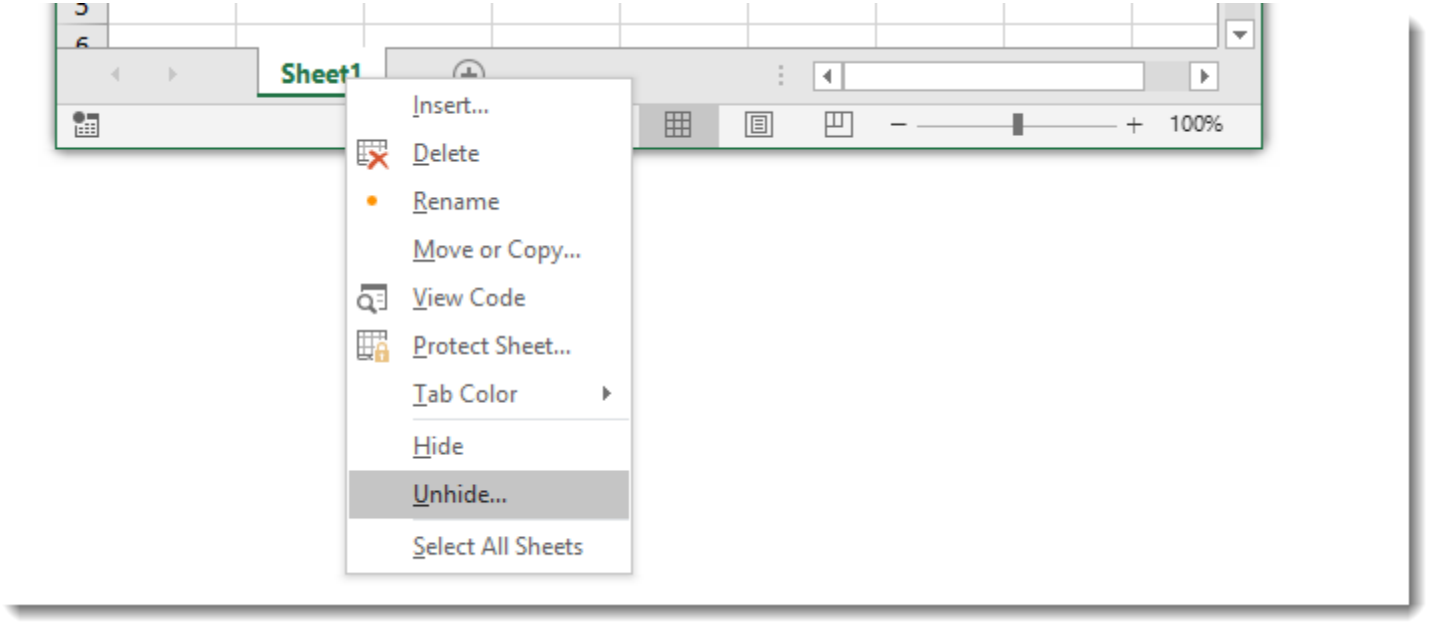
Example 3: very hidden

Tip 3: Use!



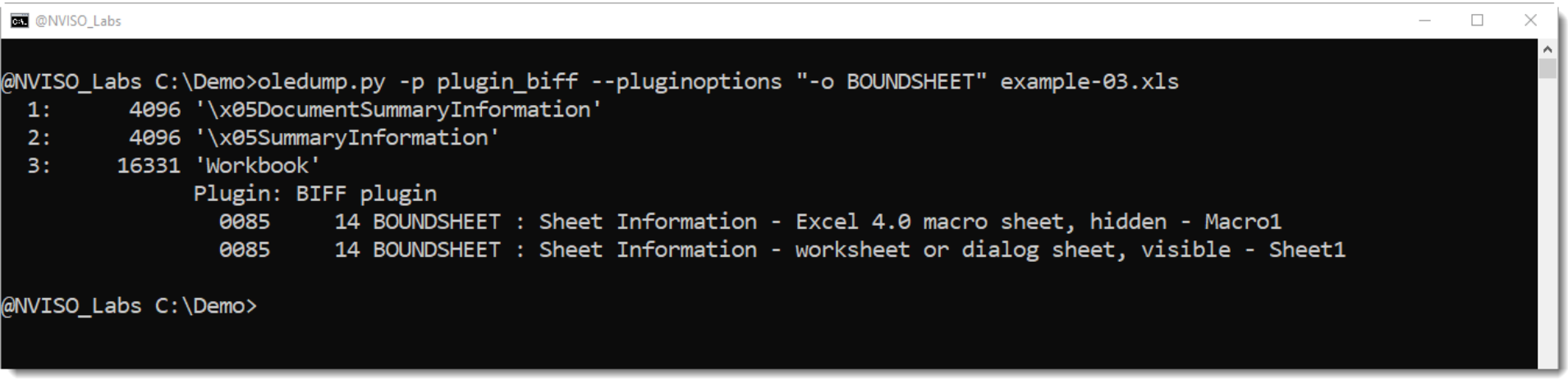
Example 3: very hidden

Tip 3: Use!



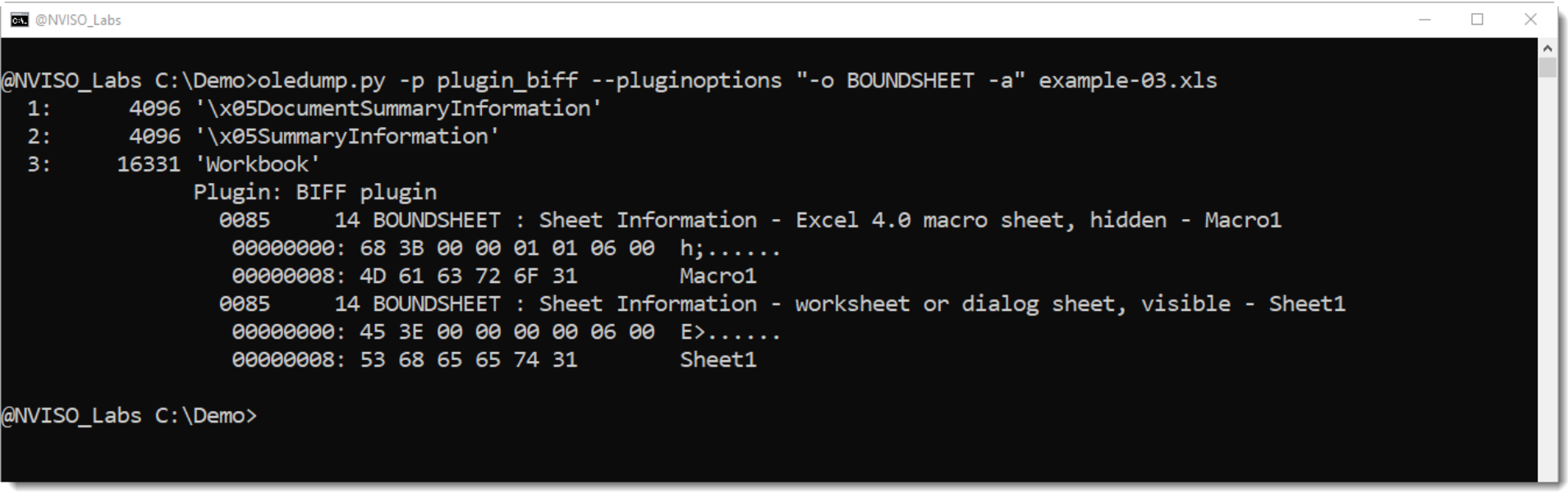
Example 3: very hidden

Tip 3: Use!



Example 3: very hidden

Tip 3: Use!

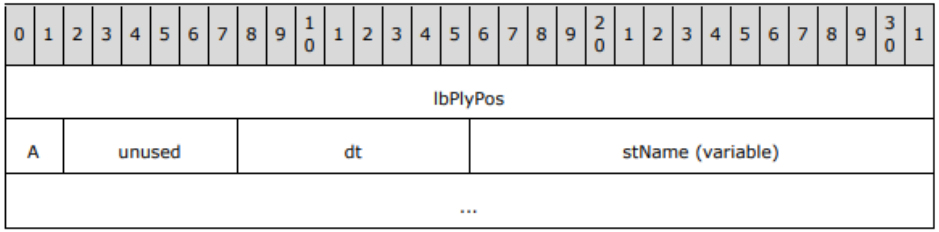


Example 3: very hidden

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).



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:

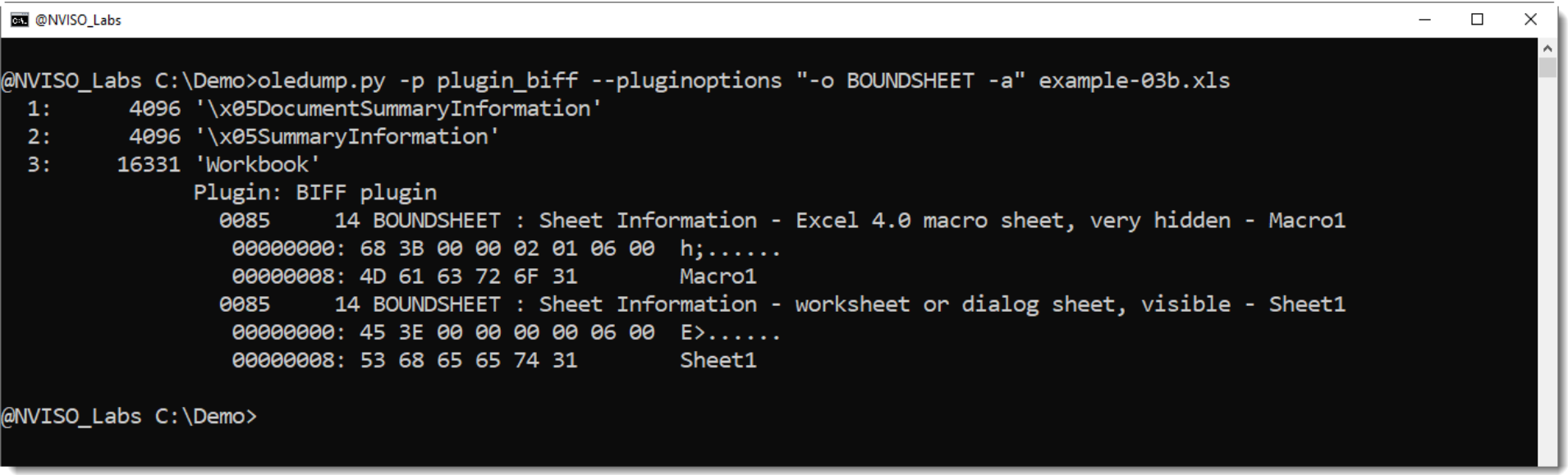
Value	Meaning
0x00	**Visible**
0x01	Hidden
0x02	Very Hidden; the sheet (1) is hidden and cannot be displayed using the user interface.

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

https://docs.microsoft.com/en-us/openspecs/office_file_formats/ms-xls/cd03cb5f-ca02-4934-a391-bb674cb8aa06

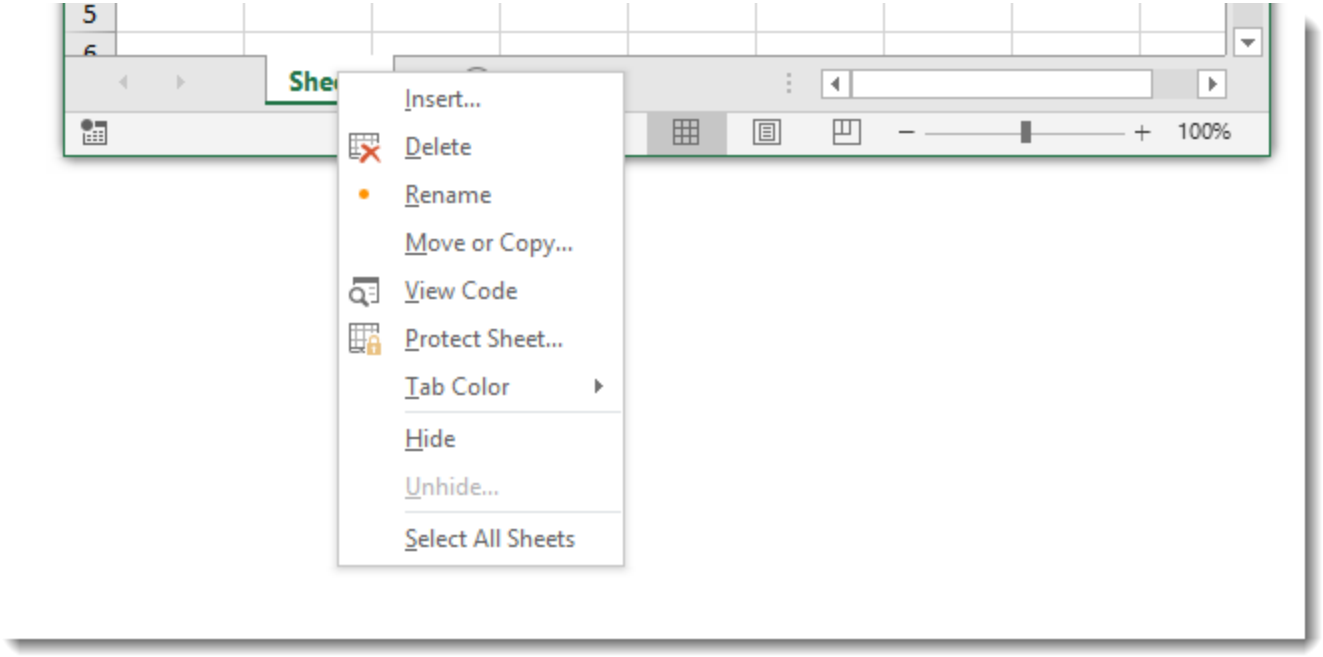
Example 3: very hidden

Tip 3: Use!



Example 3: very hidden

Tip 3: Use!

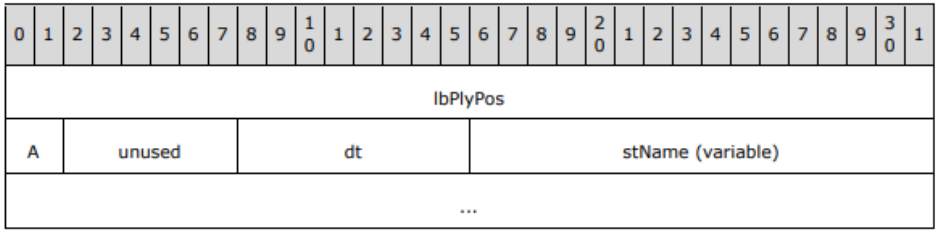


Example 4: very, very hidden?

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).



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).

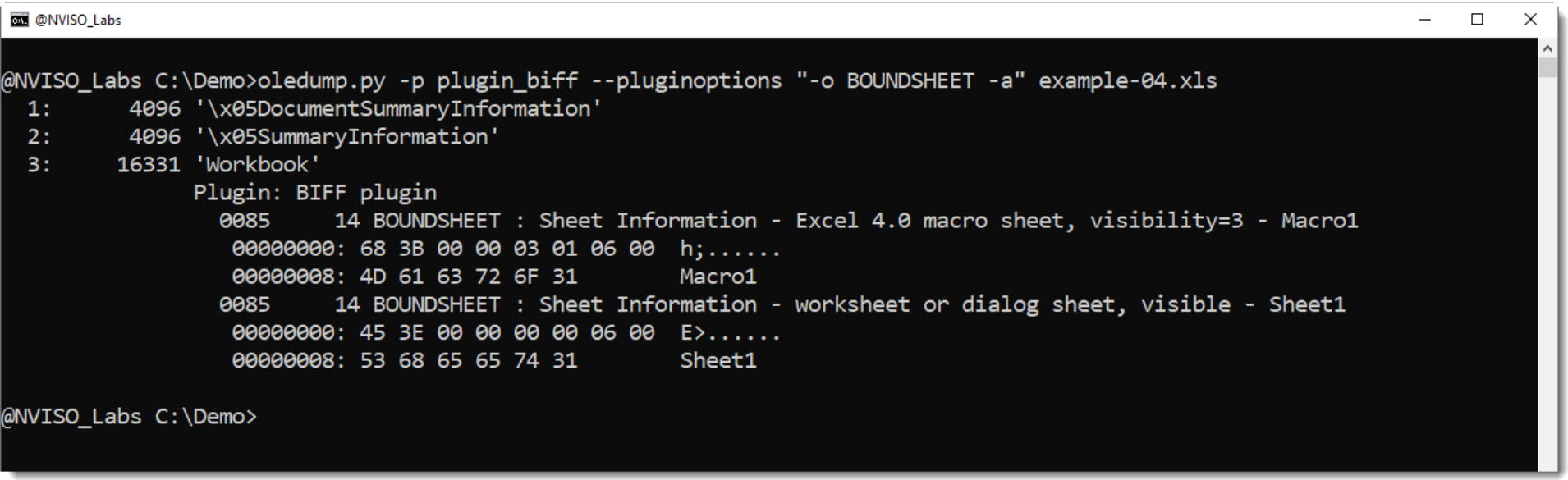
A - hsState (2 bits): An unsigned integer that specifies the hidden state of the sheet (1). MUST be a value from the following table:

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.

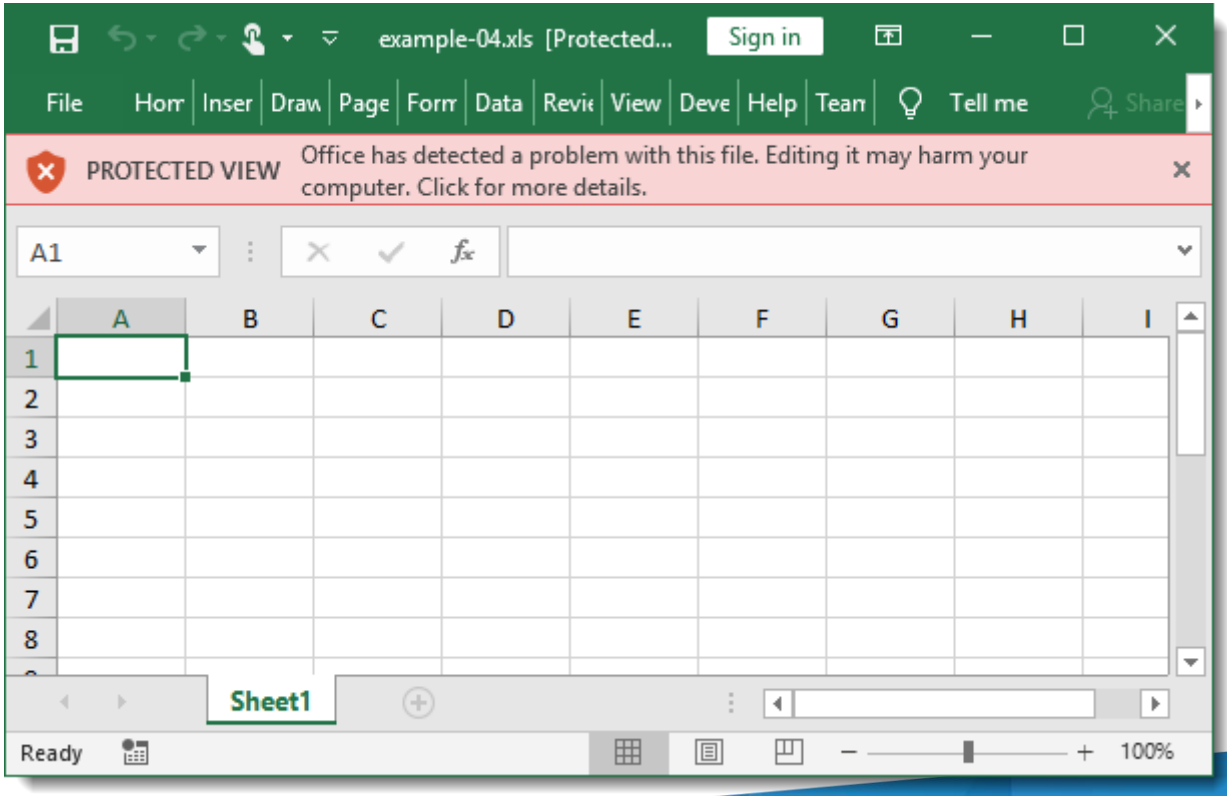
Example 4: very, very hidden?

Tip 4: Abuse!



Example 4: very, very hidden?

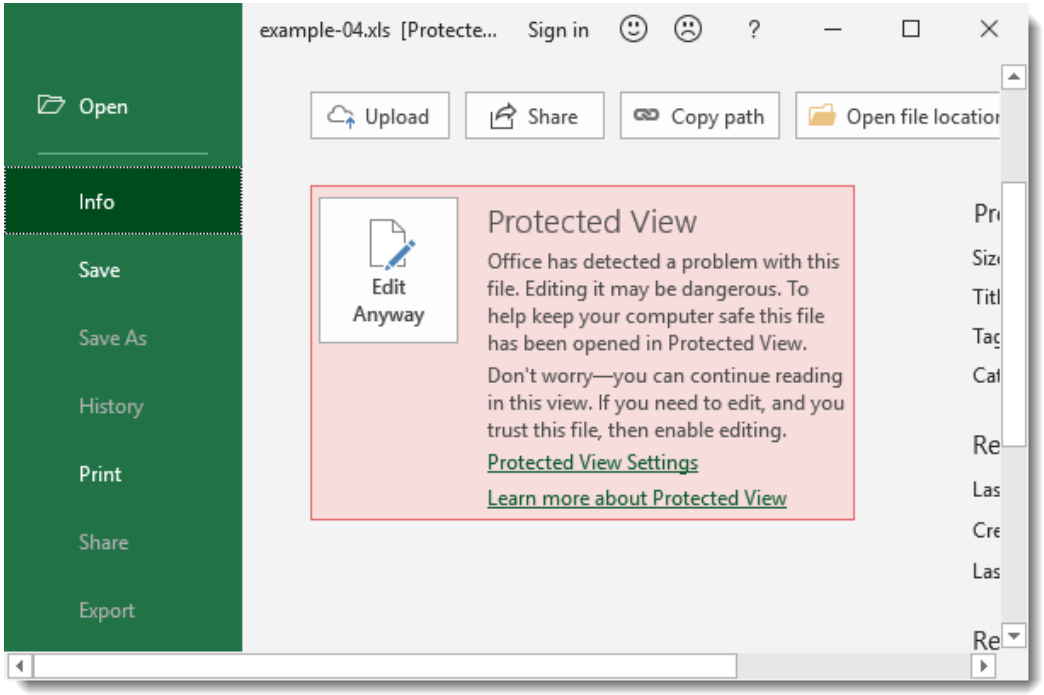
Tip 4: Abuse!



Disclosure

Example 4: very, very hidden?

Tip 4: Abuse!

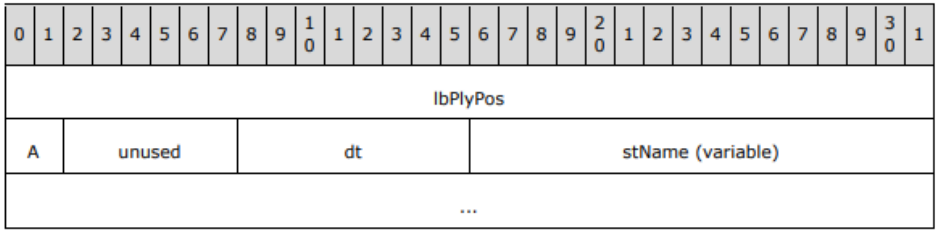


Example 5: unused bits

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).

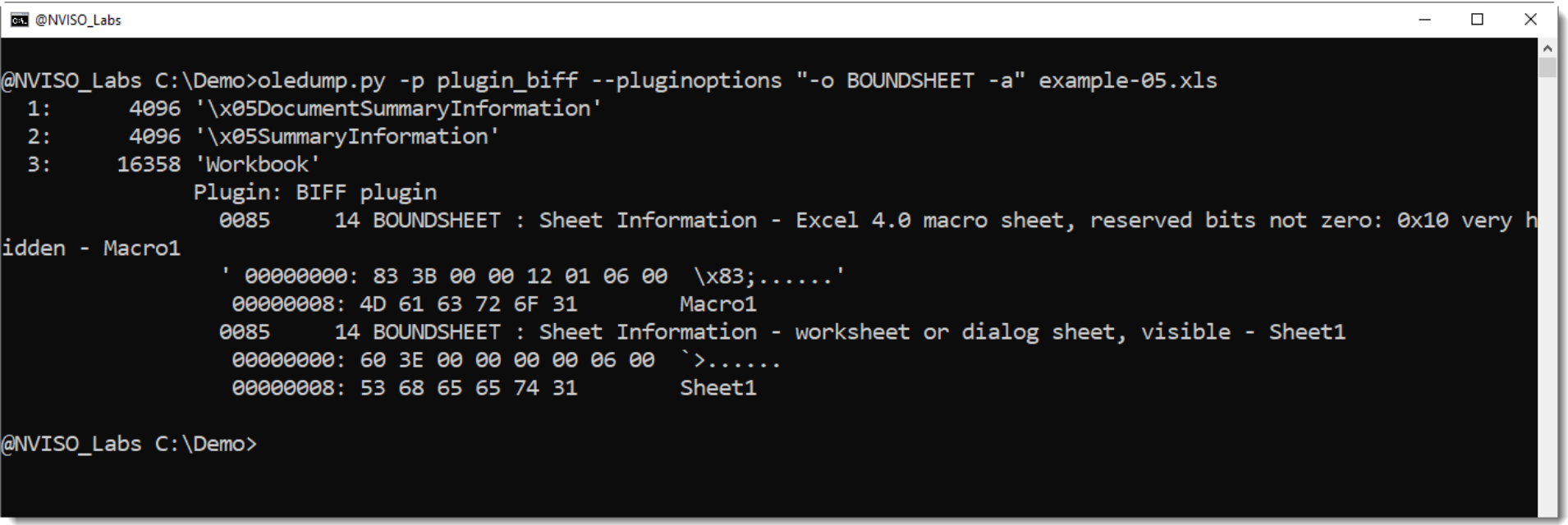
A - hsState (2 bits): An unsigned integer that specifies the hidden state of the sheet (1). MUST be a value from the following table:

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.

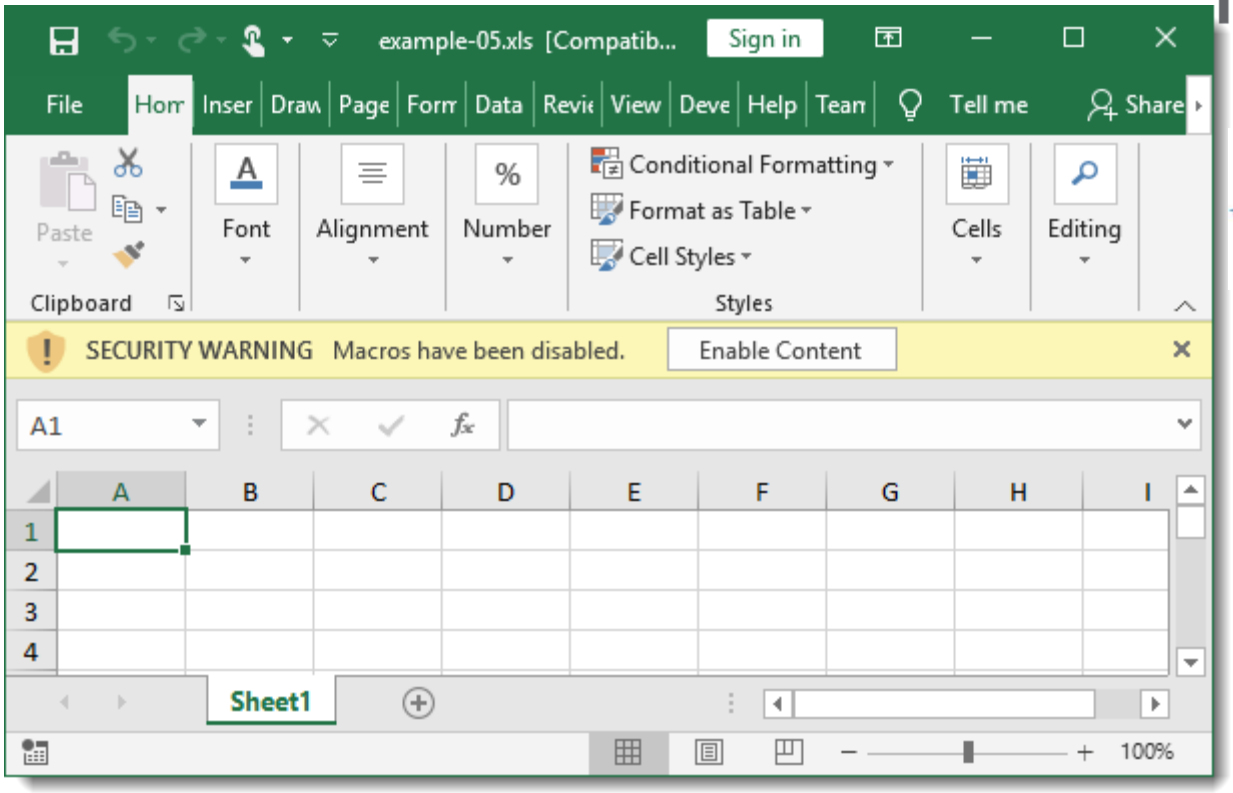
Example 5: unused bits

Tip 4: Abuse!



Example 5: unused bits

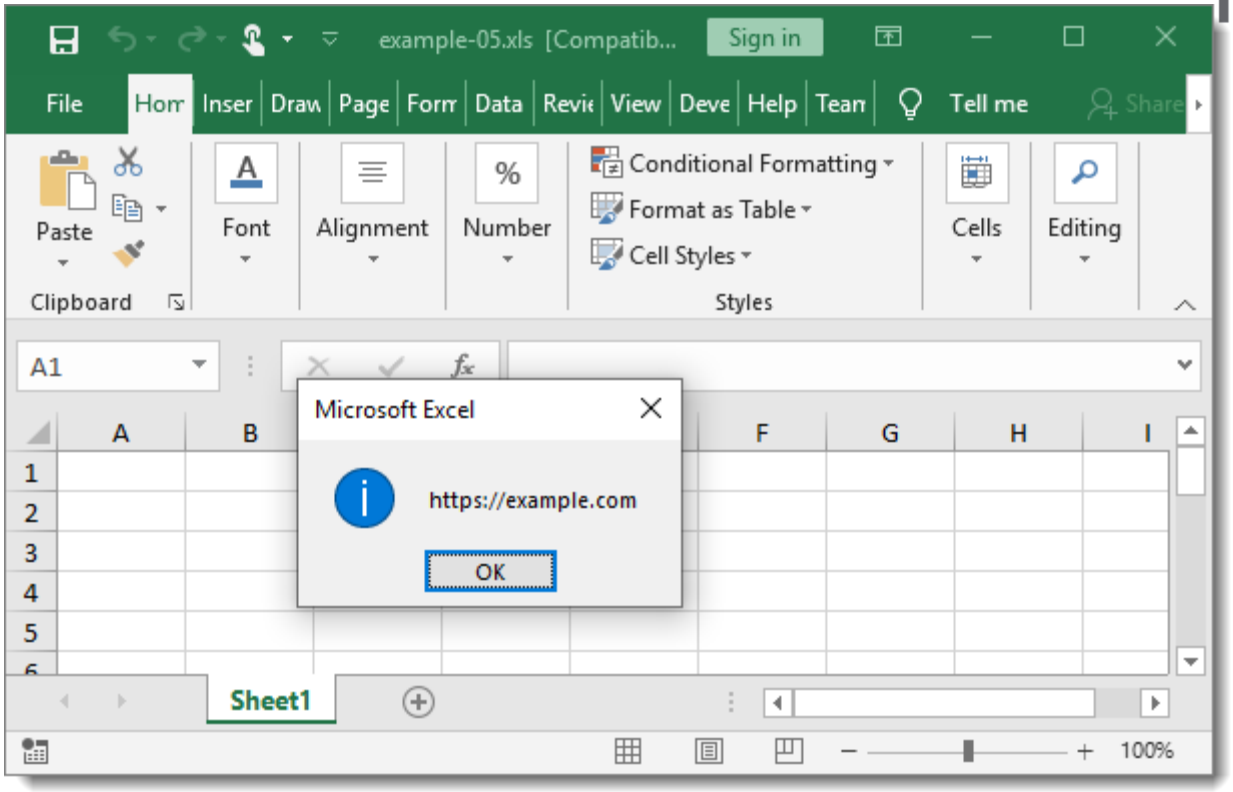
Tip 4: Abuse!



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 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 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)
}
```

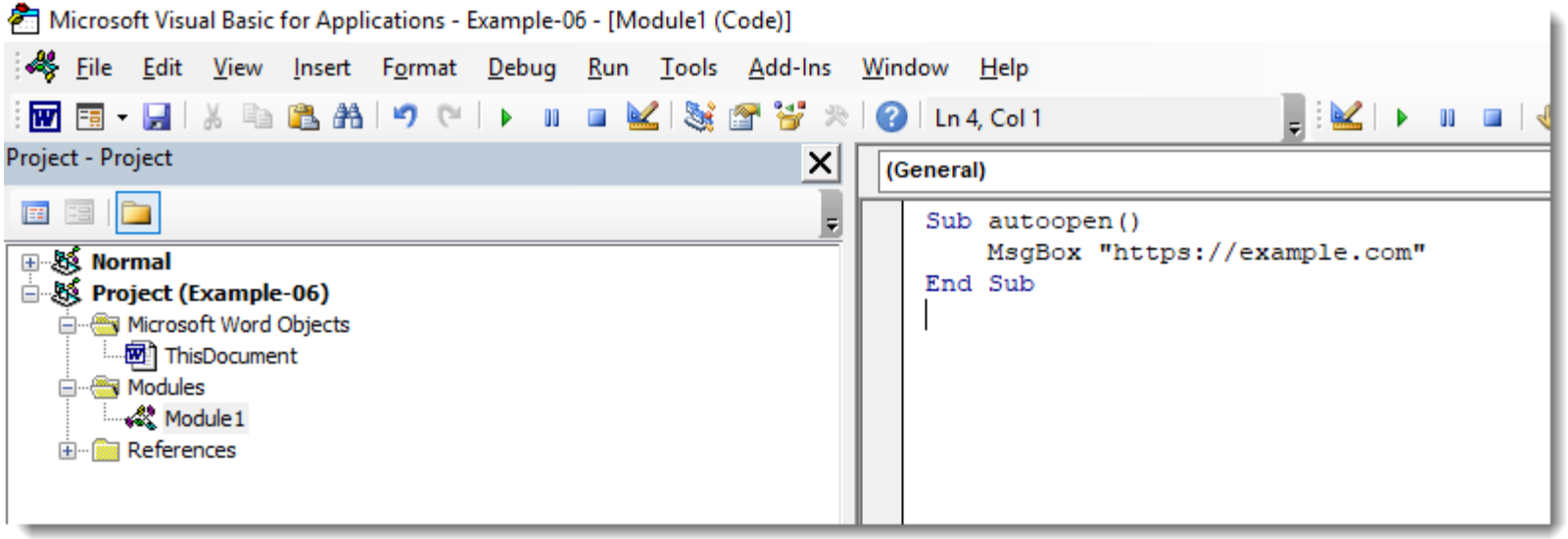
Example 5: unused bits

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 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))
}
```

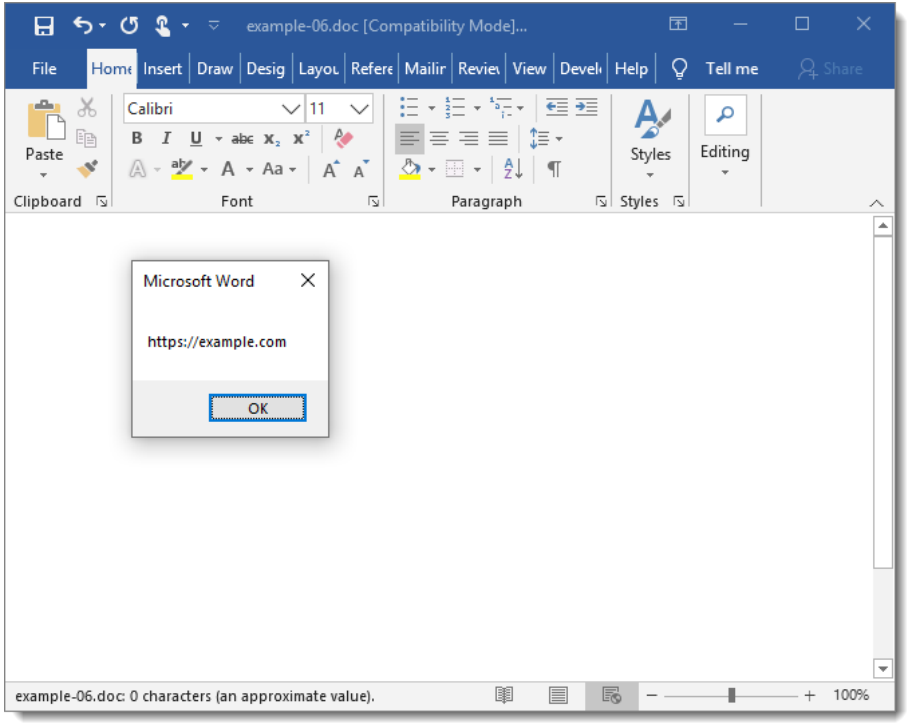
Example 6: VBA stomping

Tip 2: Learn!



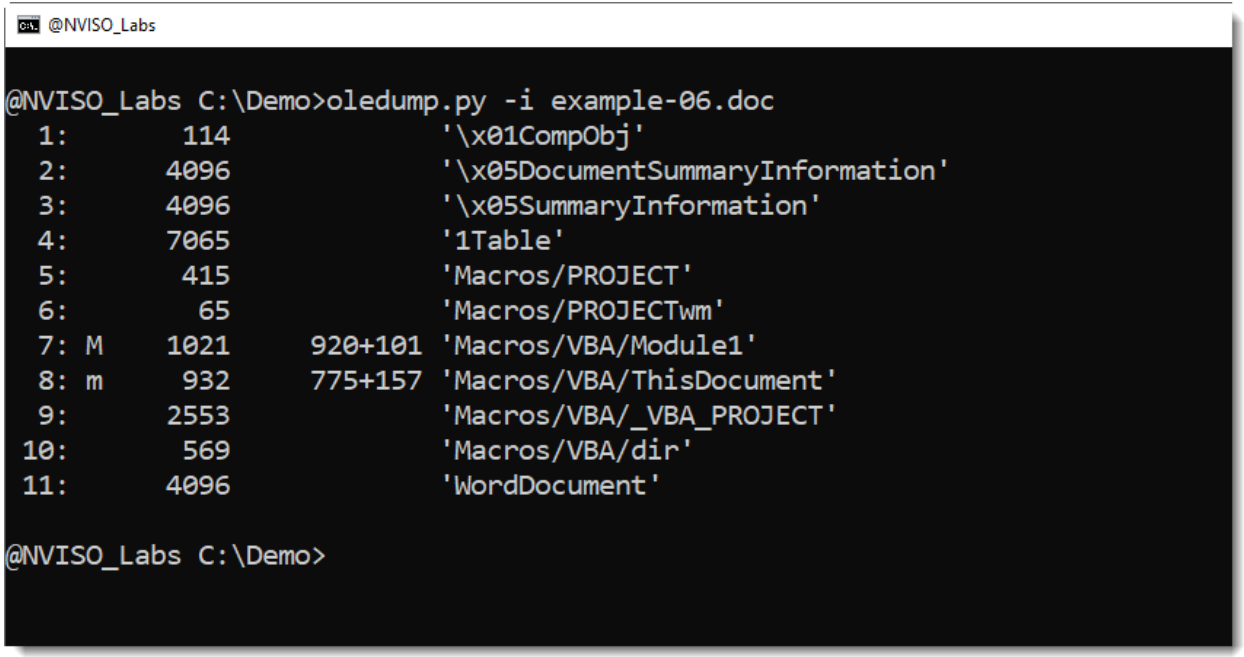
Example 6: VBA stomping

Tip 2: Learn!



Example 6: VBA stomping

Tip 2: Learn!

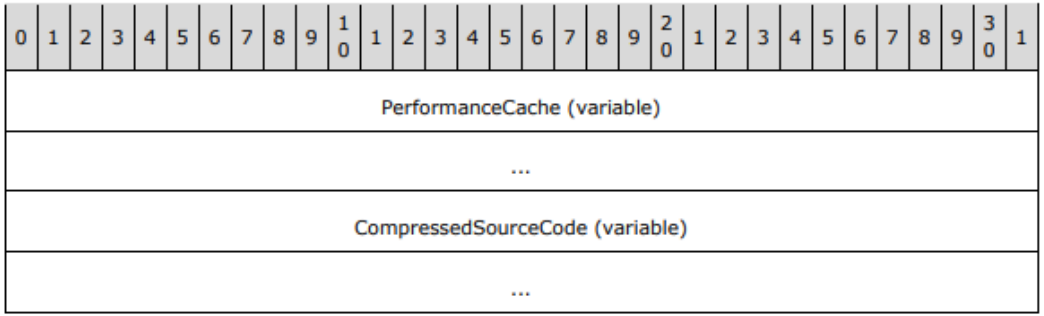


Example 6: VBA stomping

Tip 2: Learn!

2.3.4.3 Module Stream: Visual Basic Modules

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



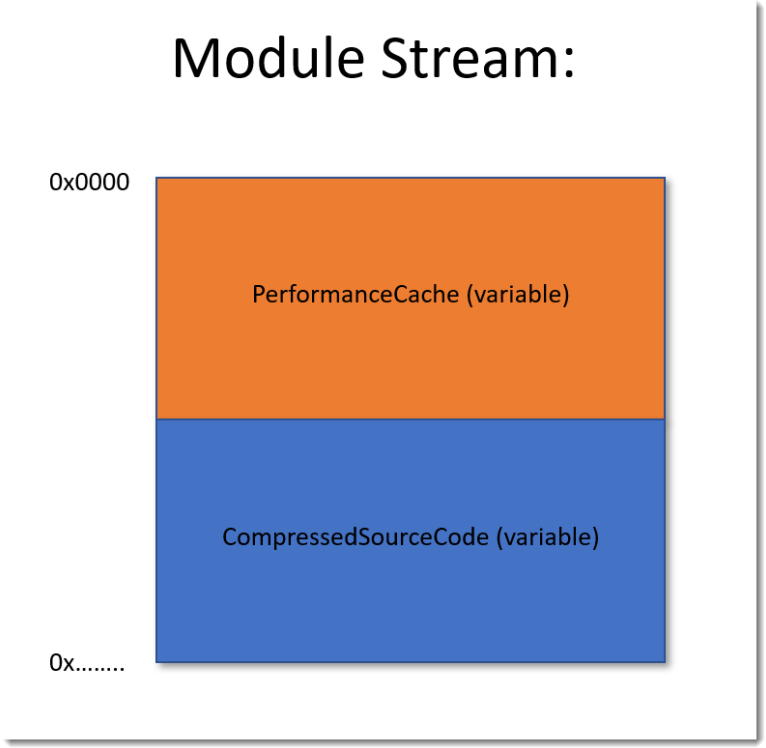
PerformanceCache (variable): An array of bytes that forms an implementation-specific and version-dependent performance cache for the module. MUST be **MODULEOFFSET** (section 2.3.4.2.3.2.5) bytes in size. MUST be ignored on read.

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).

https://docs.microsoft.com/en-us/openspecs/office_file_formats/ms-ovba/575462ba-bf67-4190-9fac-c275523c75fc

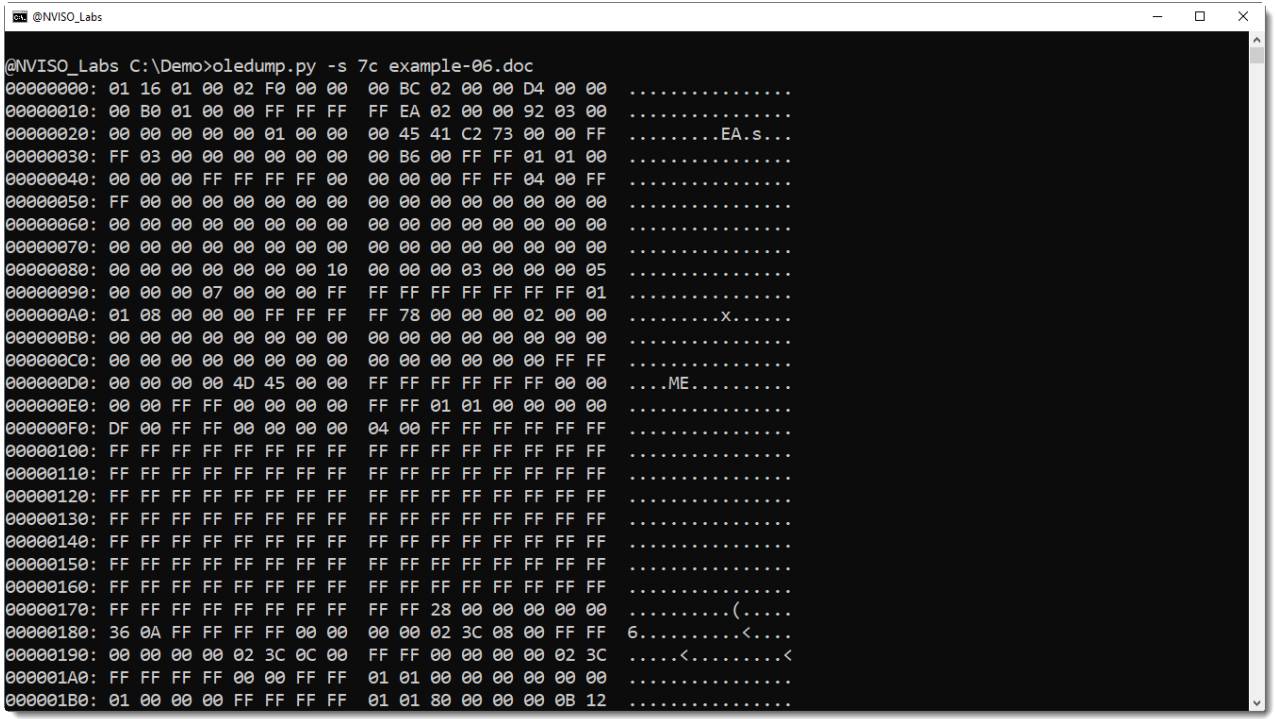
Example 6: VBA stomping

Tip 2: Learn!



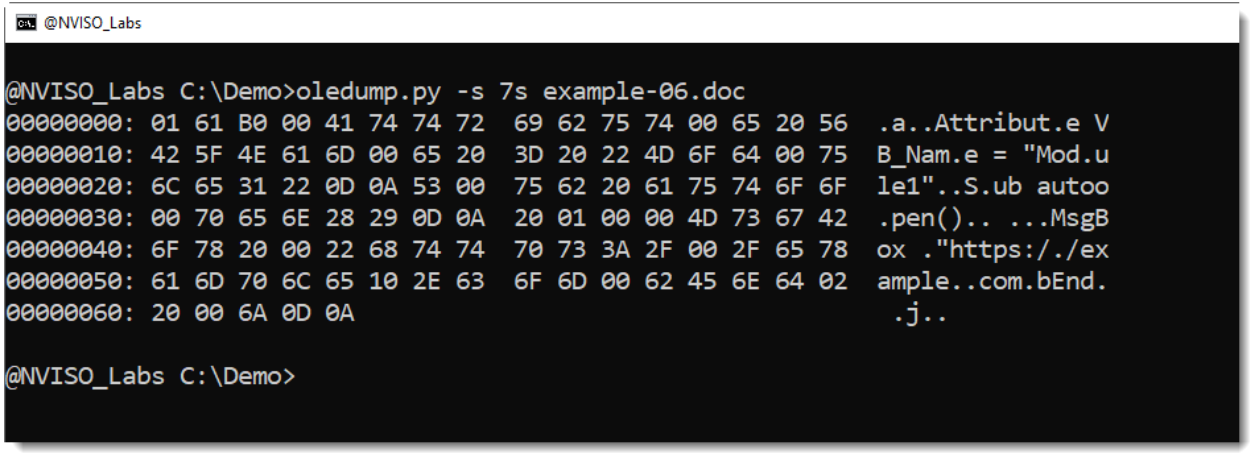
Example 6: VBA stomping

Tip 2: Learn!



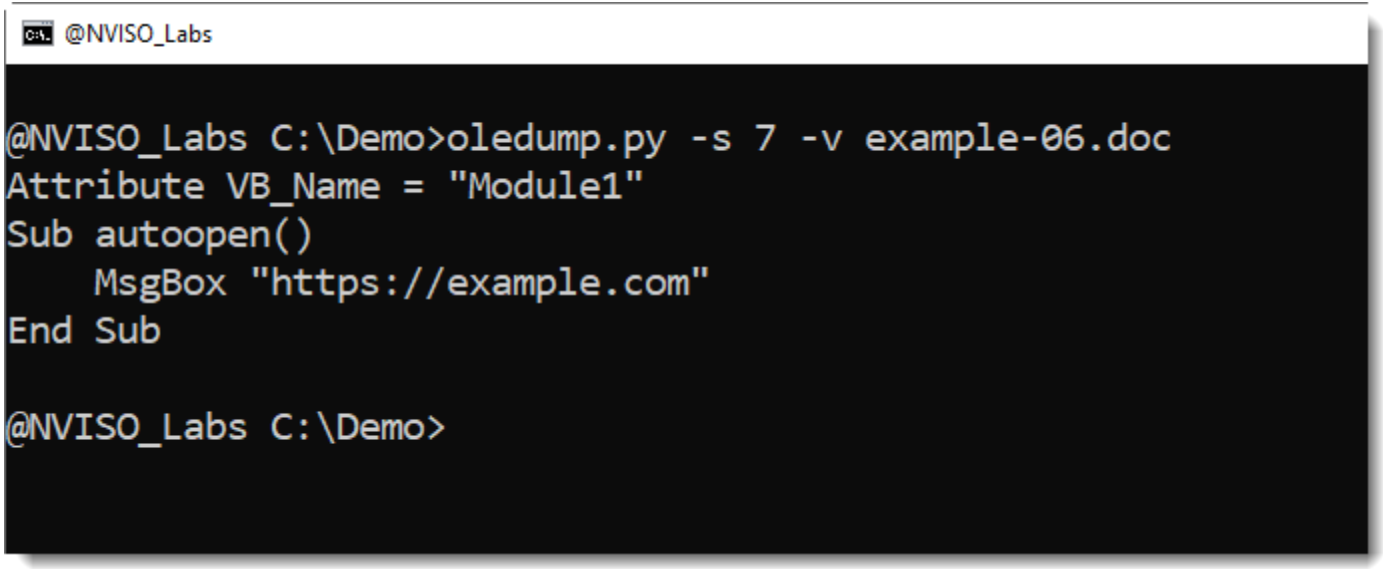
Example 6: VBA stomping

Tip 2: Learn!



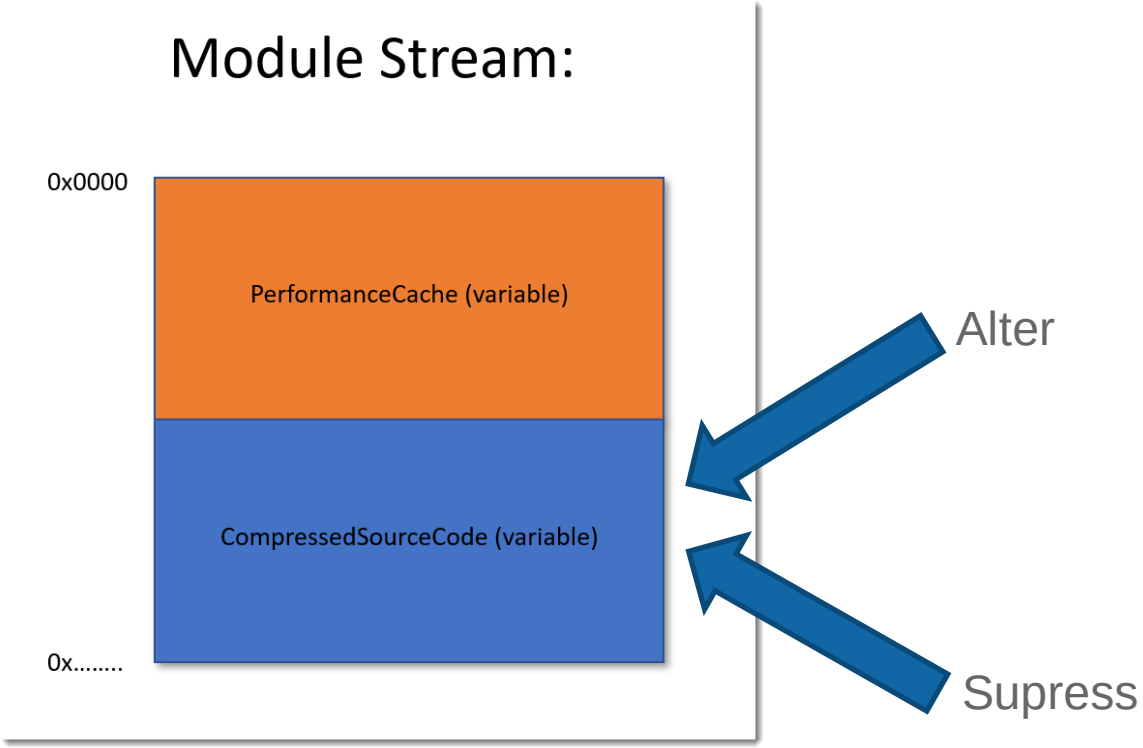
Example 6: VBA stomping

Tip 2: Learn!



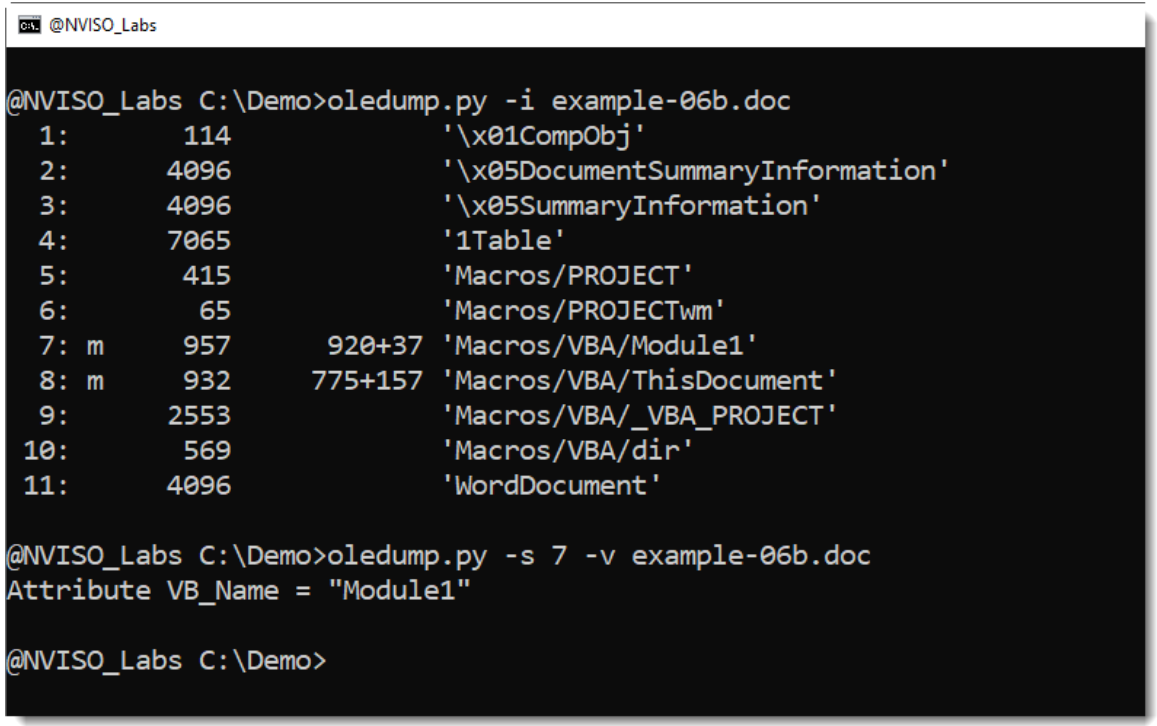
Example 6: VBA stomping

Tip 2: Learn!



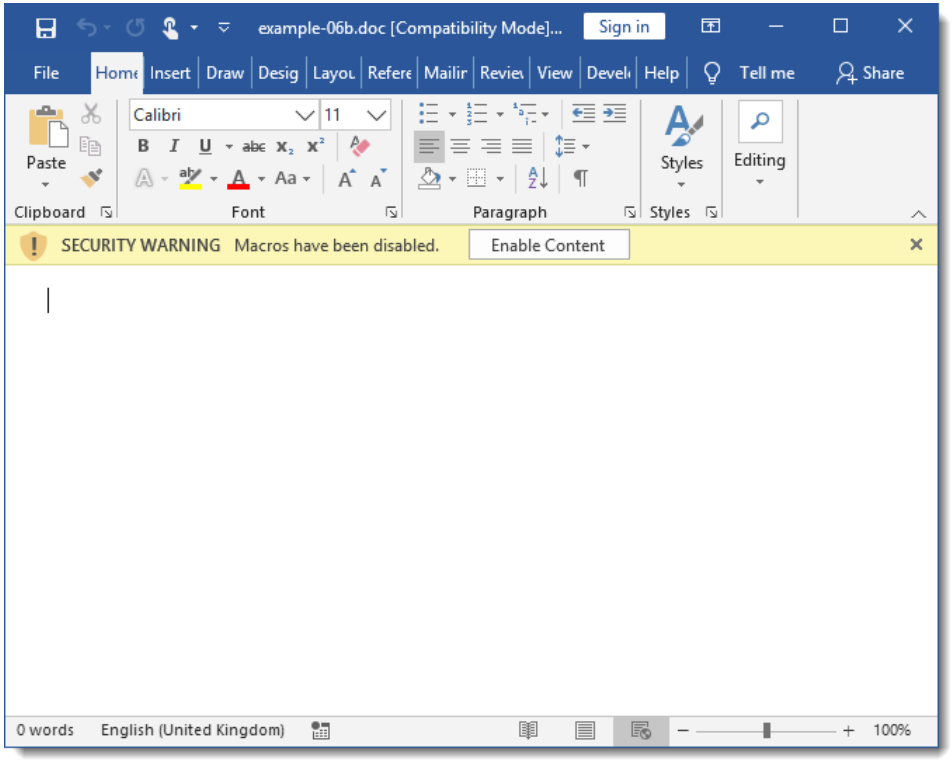
Example 6: VBA stomping

Tip 2: Learn!



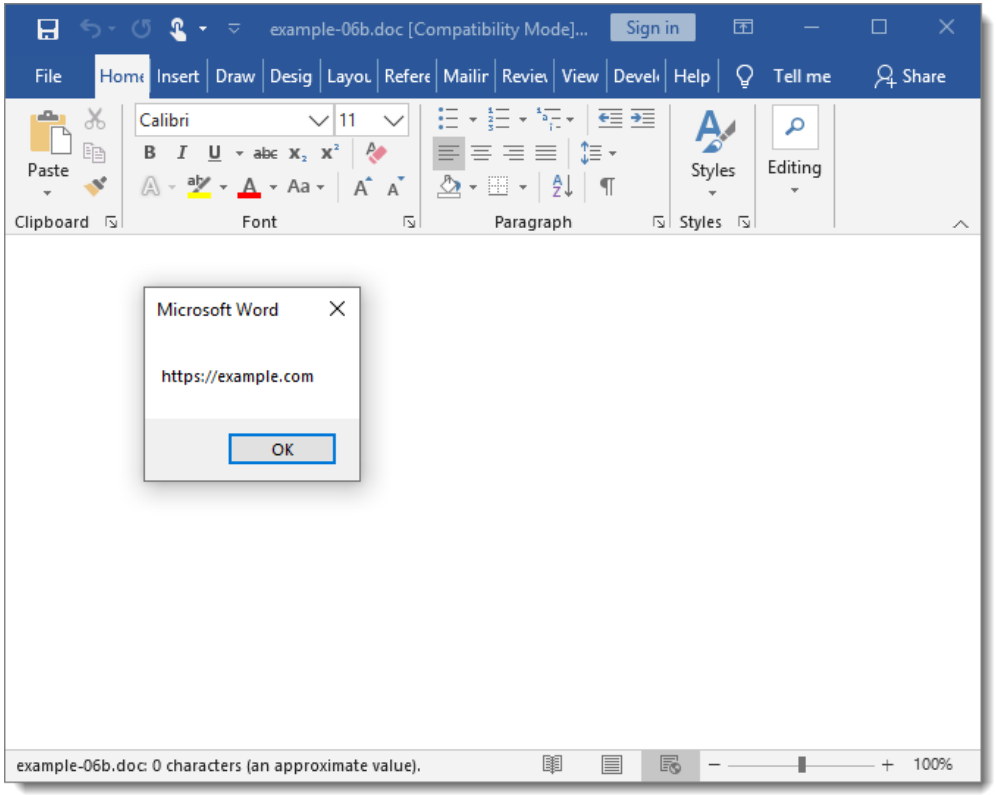
Example 6: VBA stomping

Tip 2: Learn!



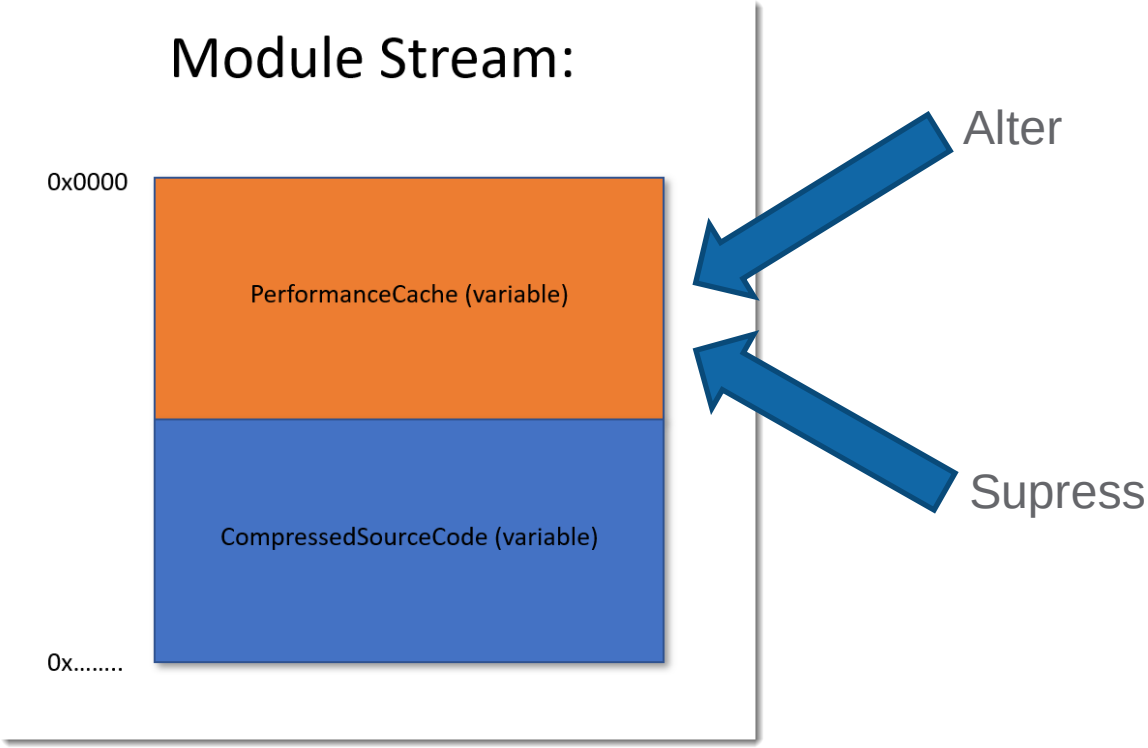
Example 6: VBA stomping

Tip 2: Learn!



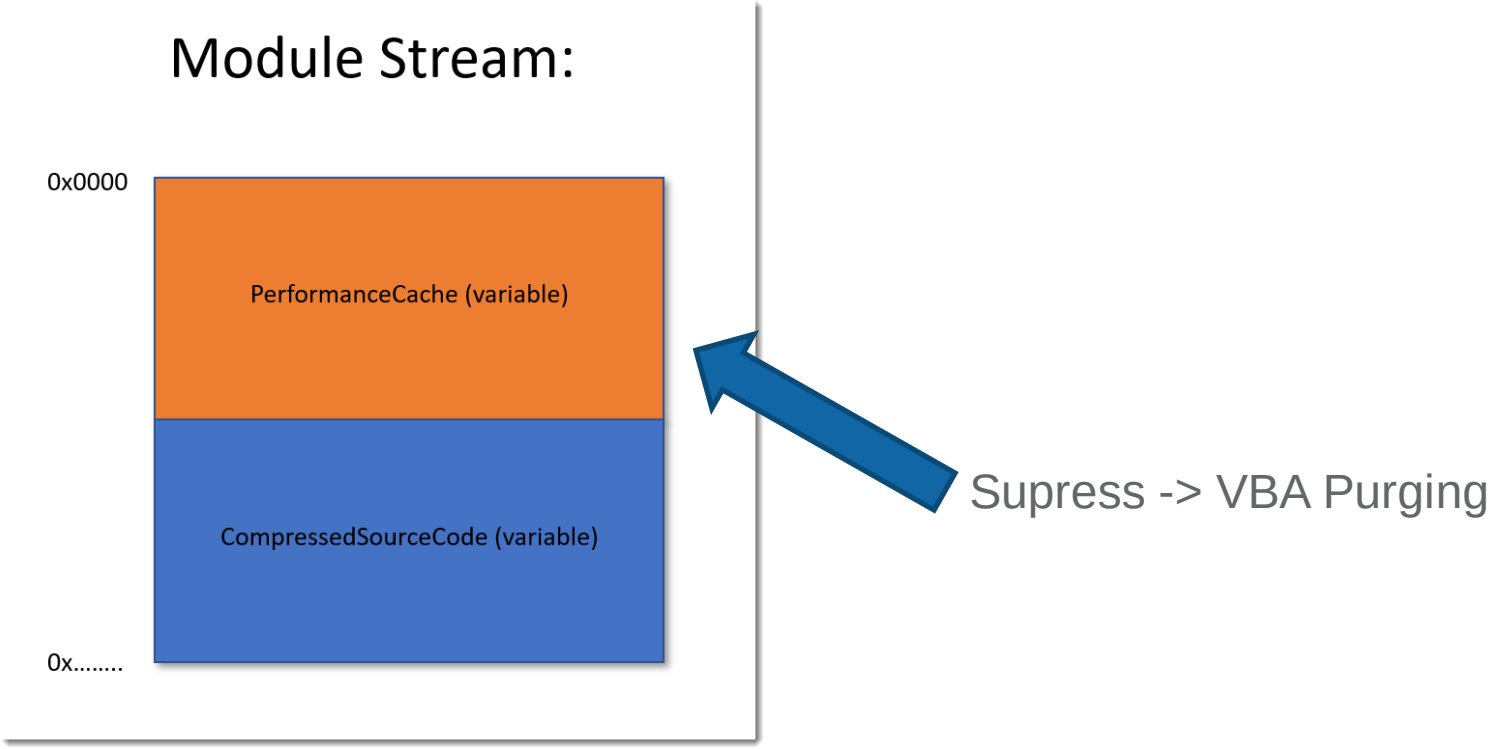
Example 7: VBA purging

Tip 3: Use!



Example 7: VBA purging

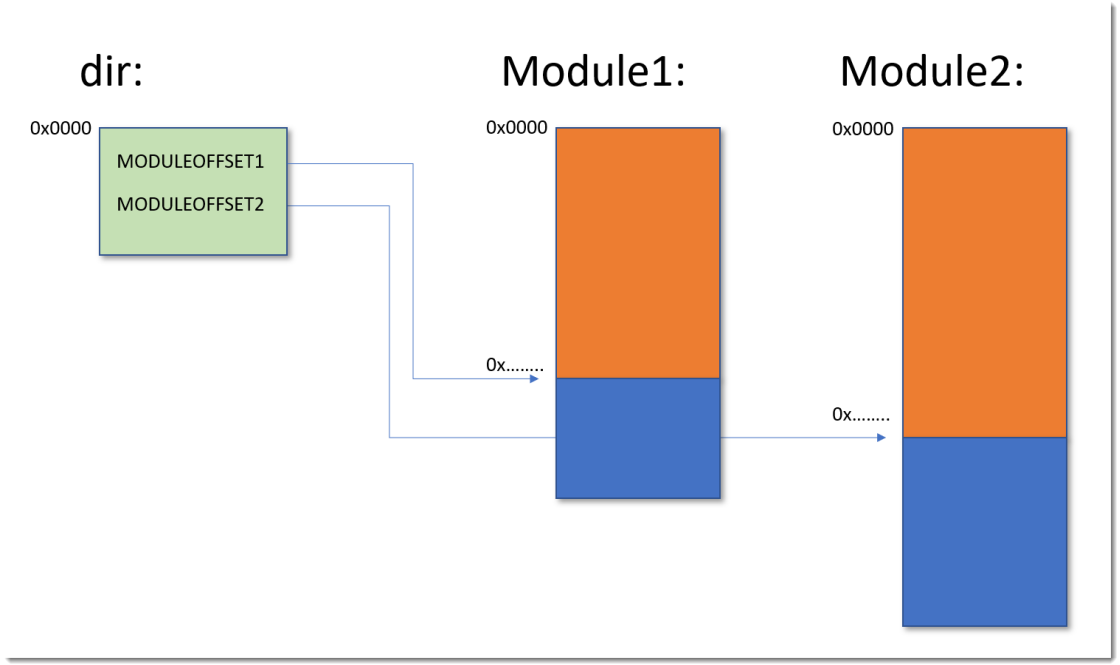
Tip 3: Use!



https://blog.nviso.eu/2020/02/25/evidence-of-vba-purging-found-in-malicious-documents/

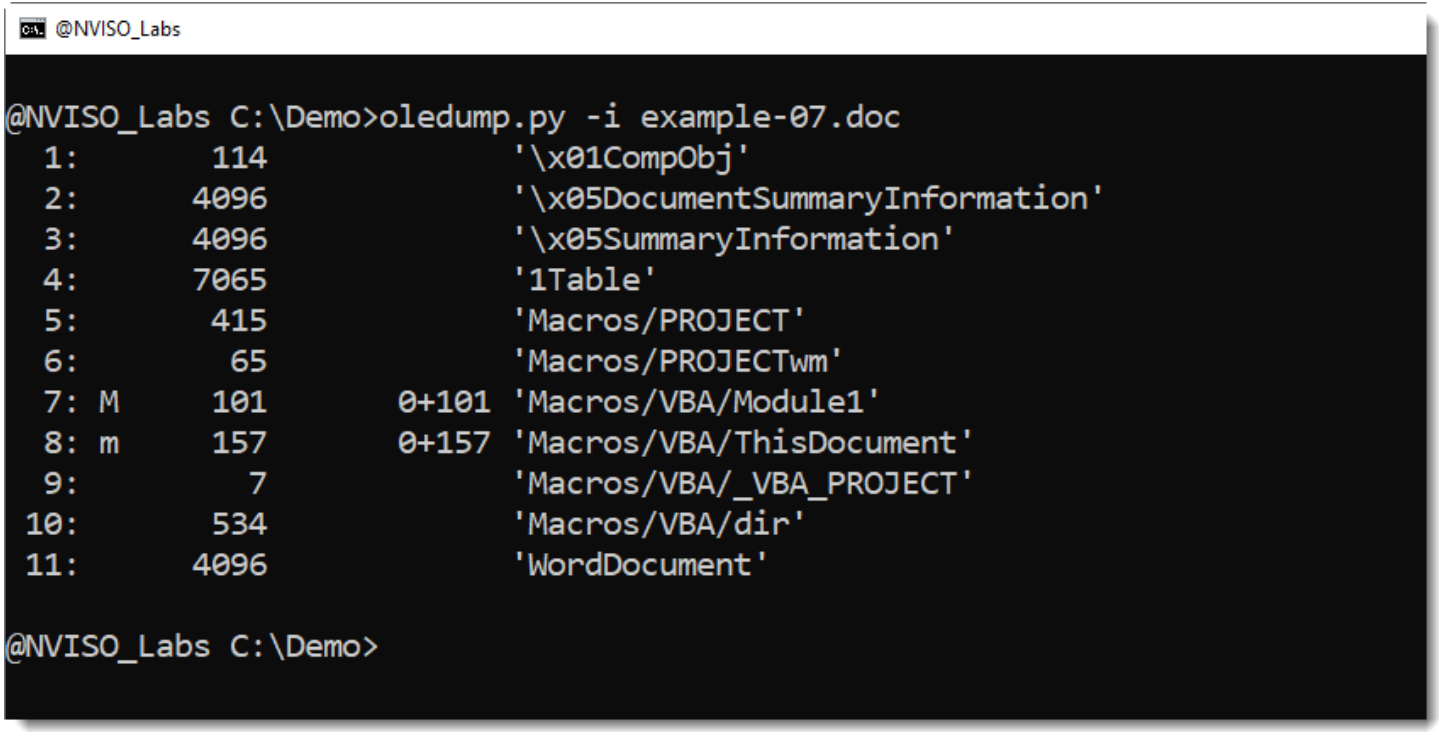
Example 7: VBA purging

Tip 3: Use!



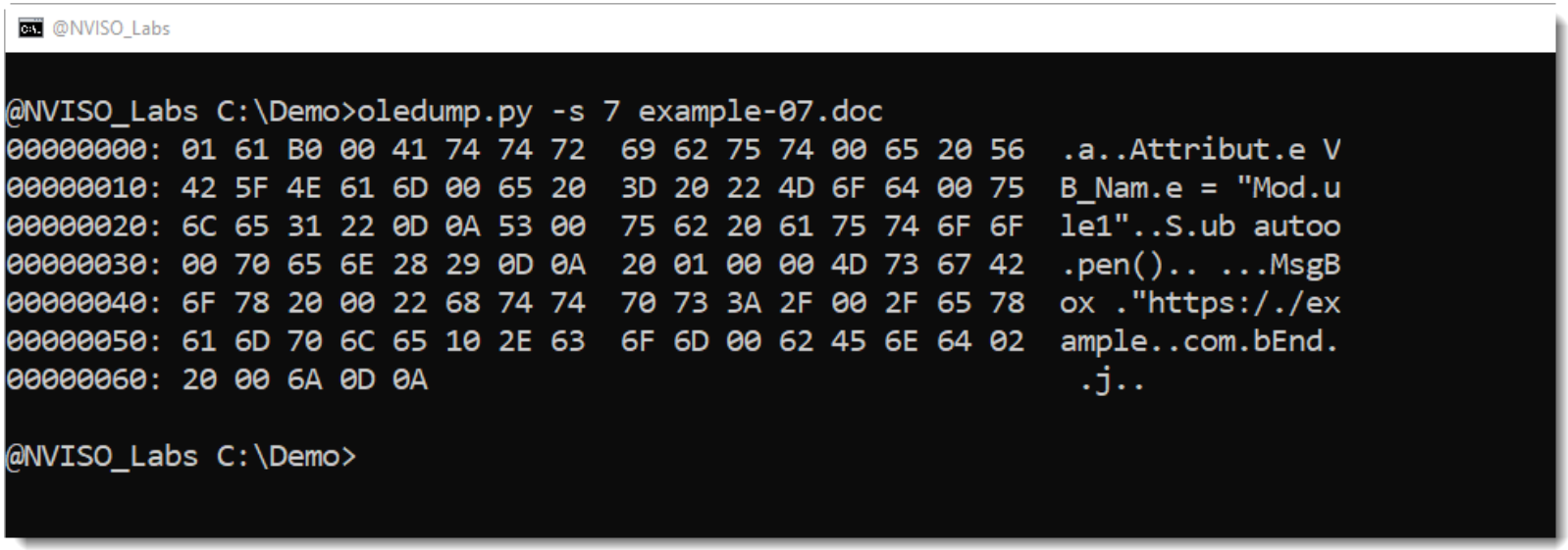
Example 7: VBA purging

Tip 3: Use!



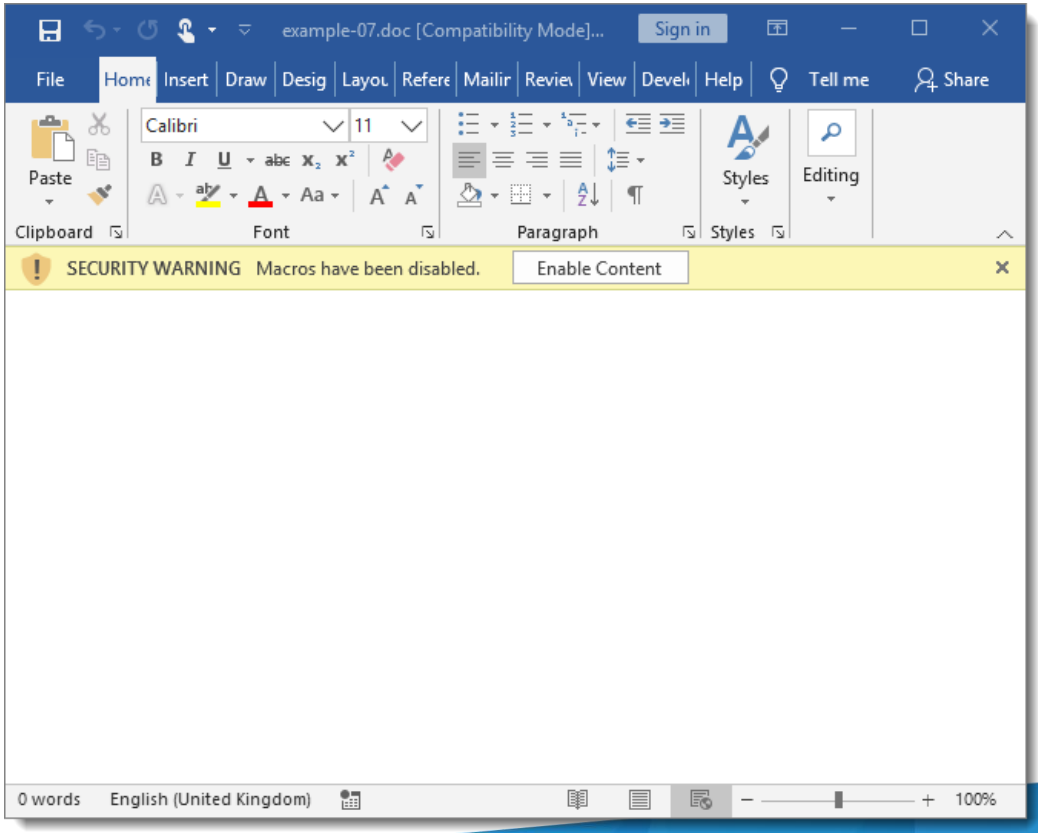
Example 7: VBA purging

Tip 3: Use!



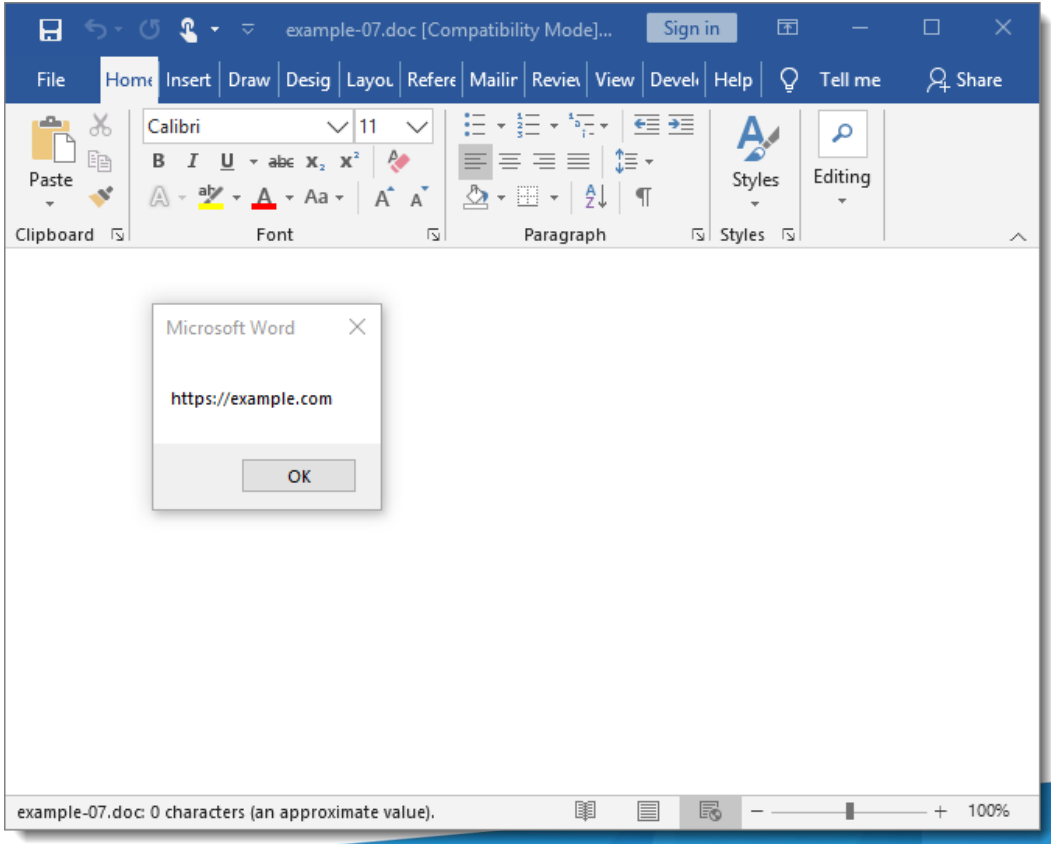
Example 7: VBA purging

Tip 3: Use!



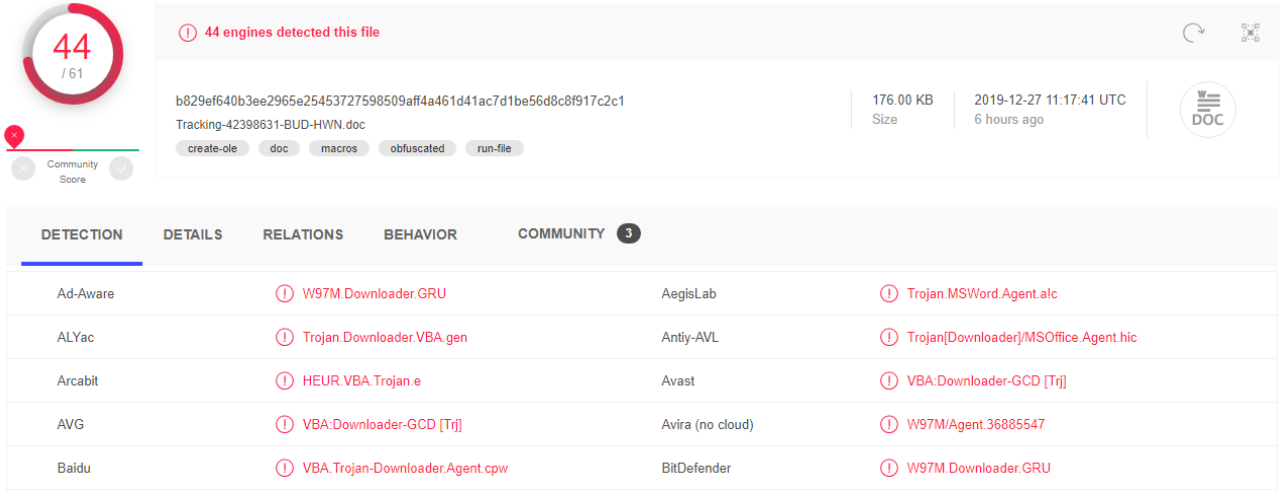
Example 7: VBA purging

Tip 3: Use!



Example 7: VBA purging

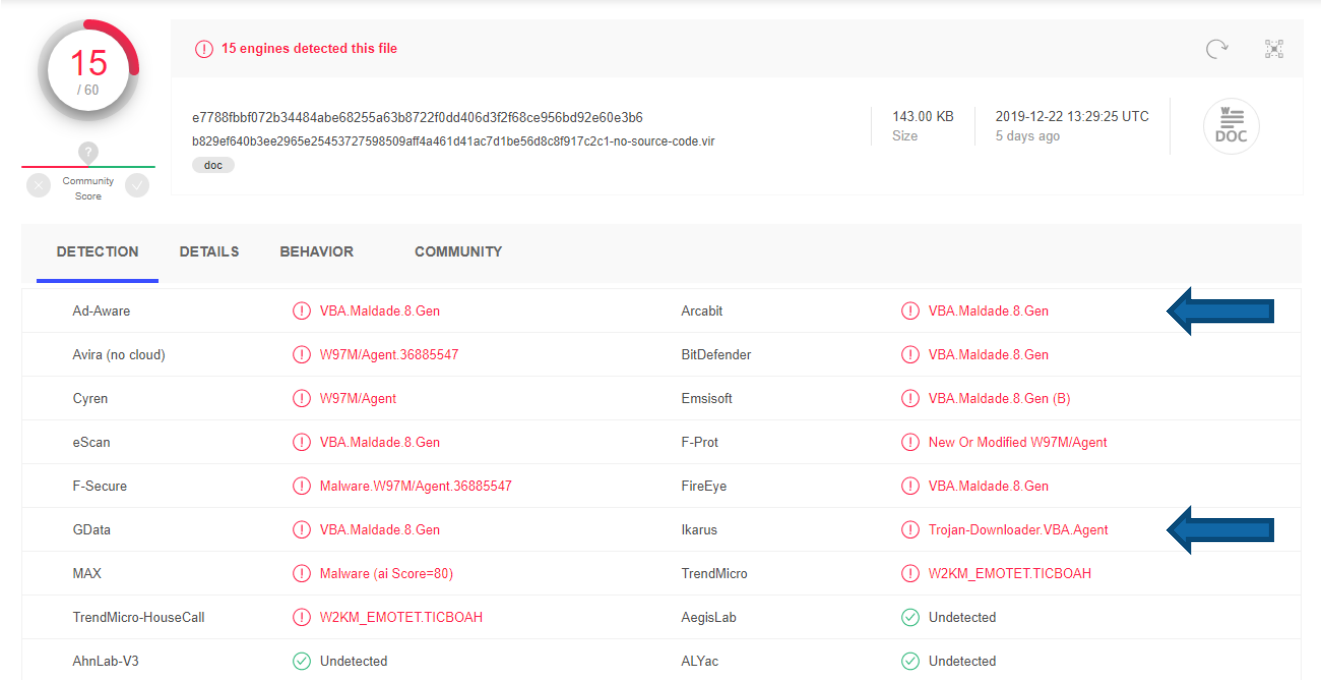
Tip 3: Use!



https://www.virustotal.com/gui/file/b829ef640b3ee2965e25453727598509aff4a461d41ac7d1be56d8c8f917c2c1/detection

Example 7: VBA purging

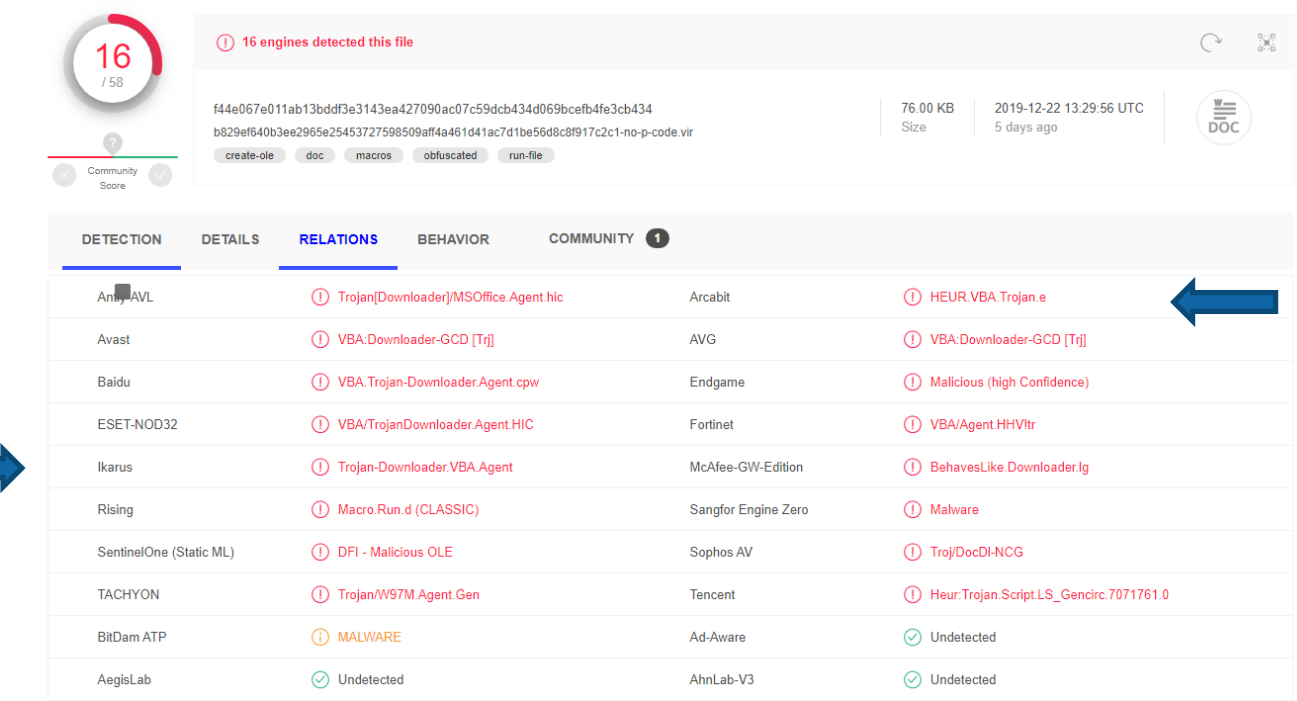
Tip 3: Use!



https://www.virustotal.com/gui/file/e7788fbbf072b34484abe68255a63b8722f0dd406d3f2f68ce956bd92e60e3b6/detection

Example 7: VBA purging

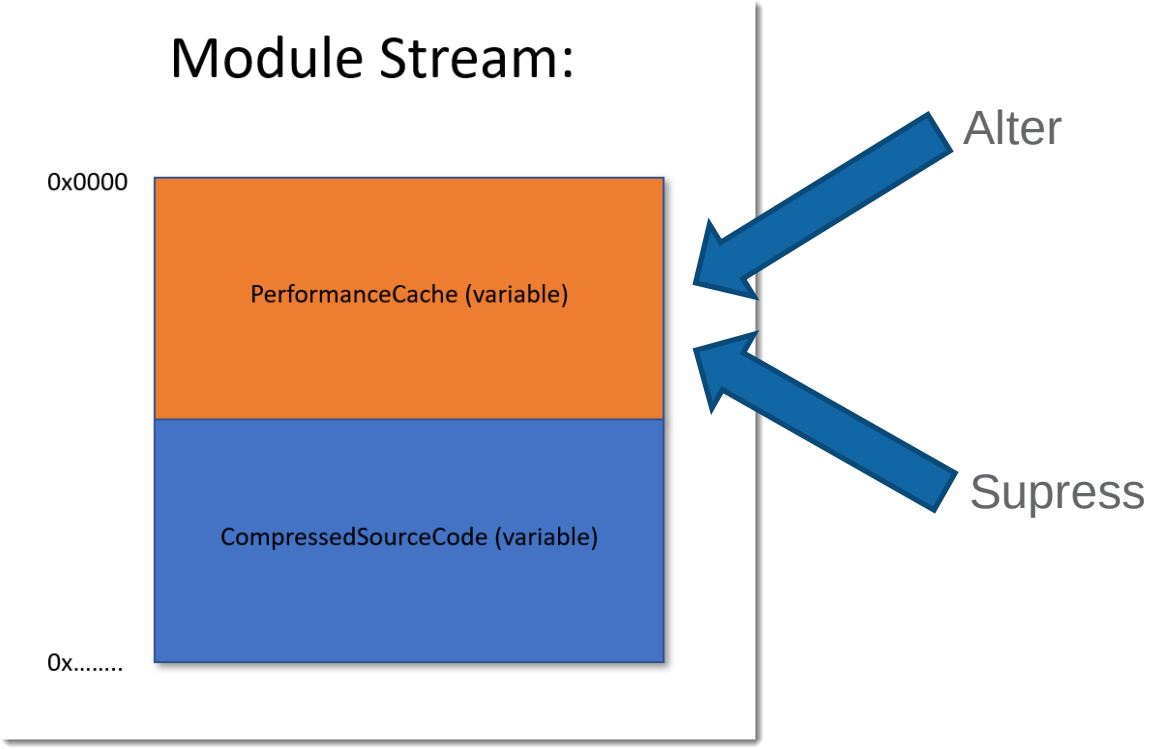
Tip 3: Use!



https://www.virustotal.com/gui/file/f44e067e011ab13bddf3e3143ea427090ac07c59dcb434d069bcefb4fe3cb434/detection

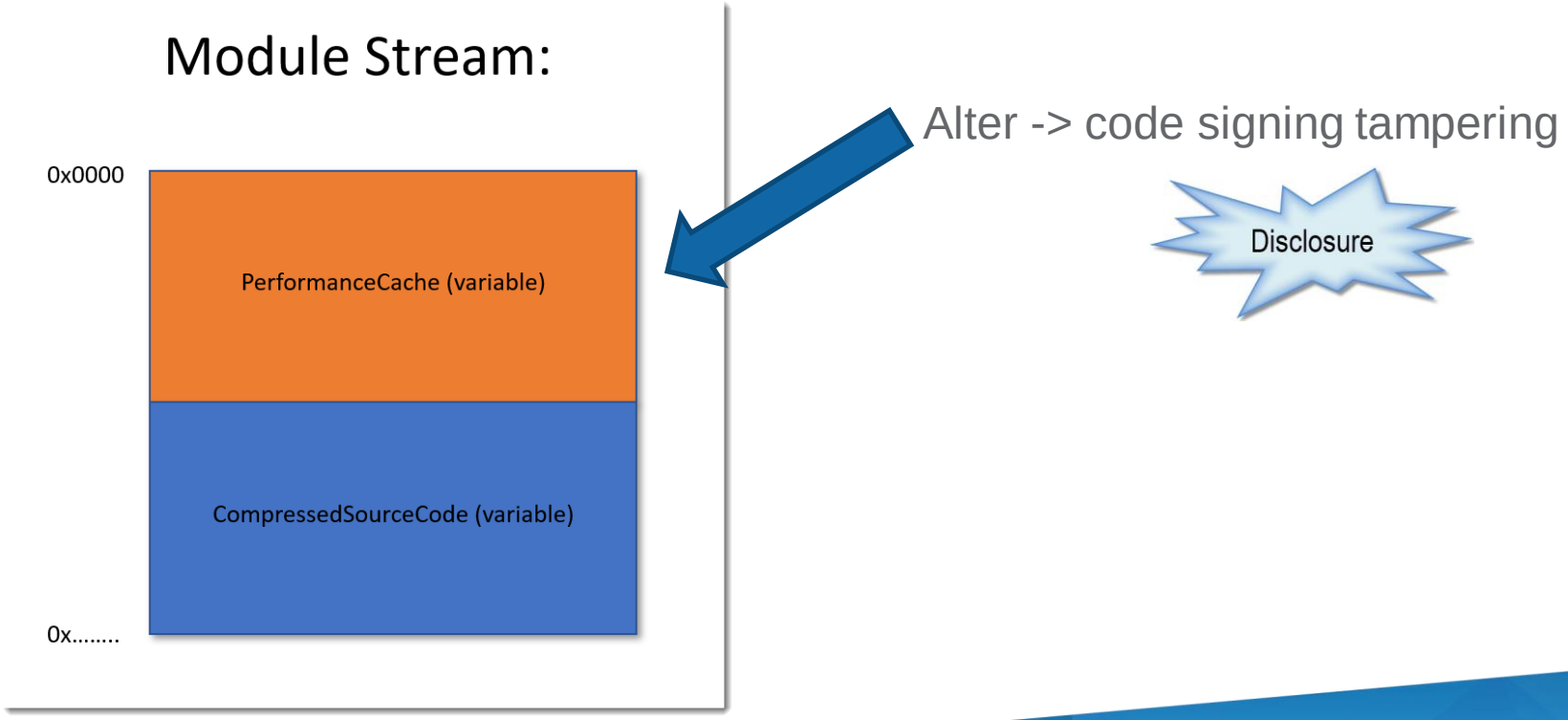
Example 8: Code signing tampering

Tip 4: Abuse!



Example 8: Code signing tampering

Tip 4: Abuse!



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.

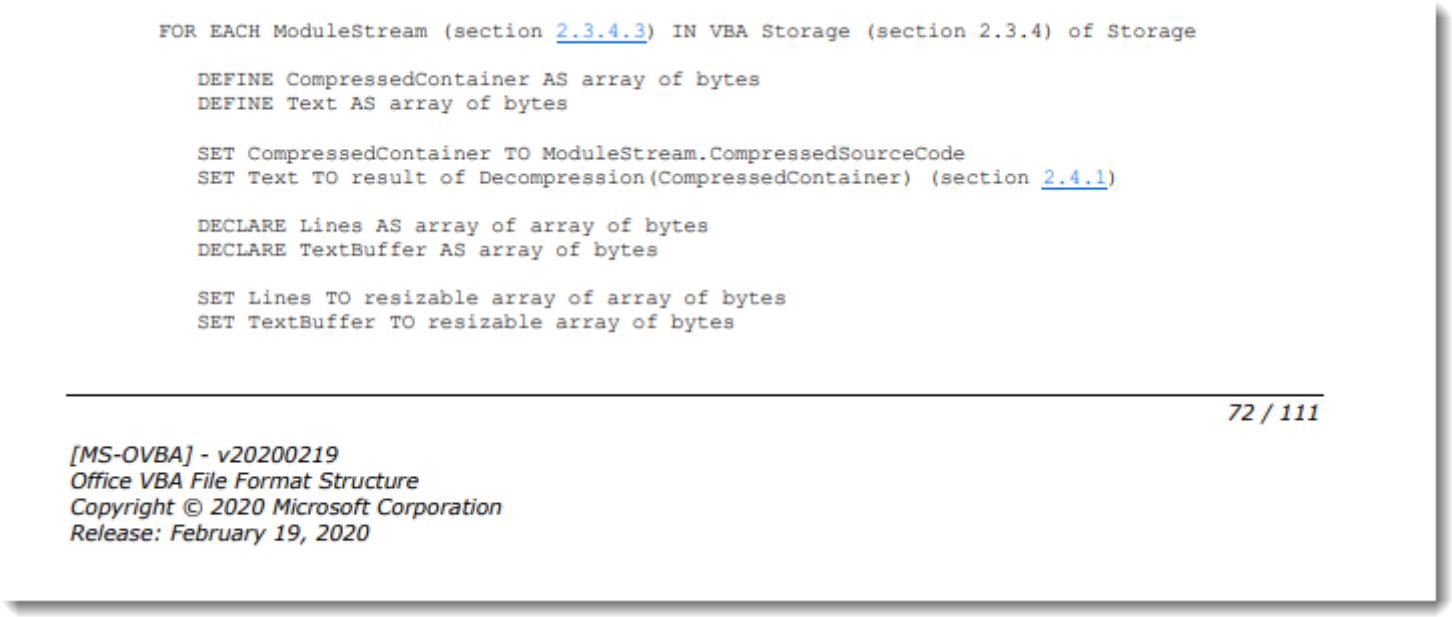
This Contents Hash algorithm requires one parameter as input:

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

https://docs.microsoft.com/en-us/openspecs/office_file_formats/ms-ovba/575462ba-bf67-4190-9fac-c275523c75fc

Example 8: Code signing tampering

Tip 4: Abuse!

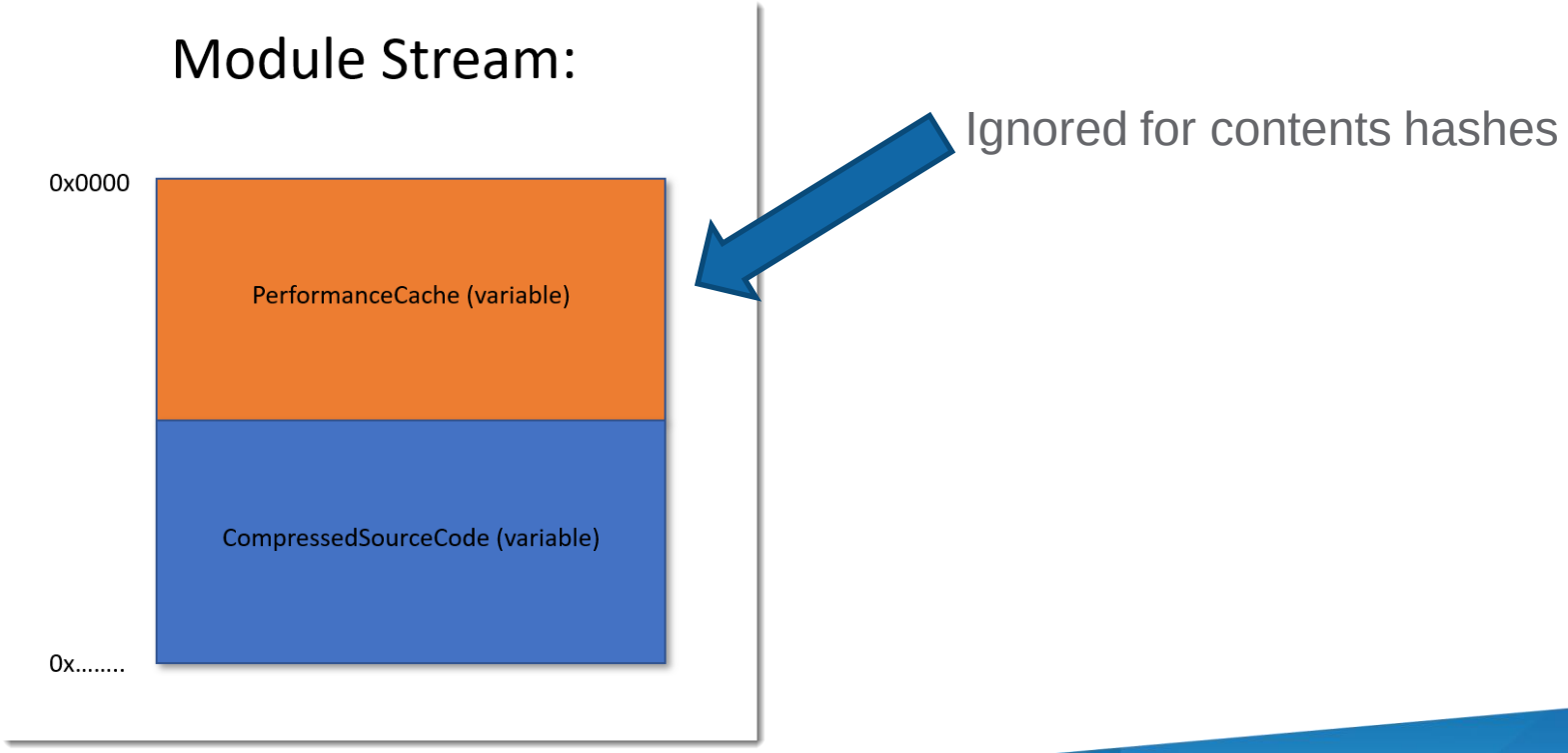


```
FOR EACH ModuleStream (section 2.3.4.3) IN VBA Storage (section 2.3.4) of Storage

   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
```


https://docs.microsoft.com/en-us/openspecs/office_file_formats/ms-ovba/575462ba-bf67-4190-9fac-c275523c75fc

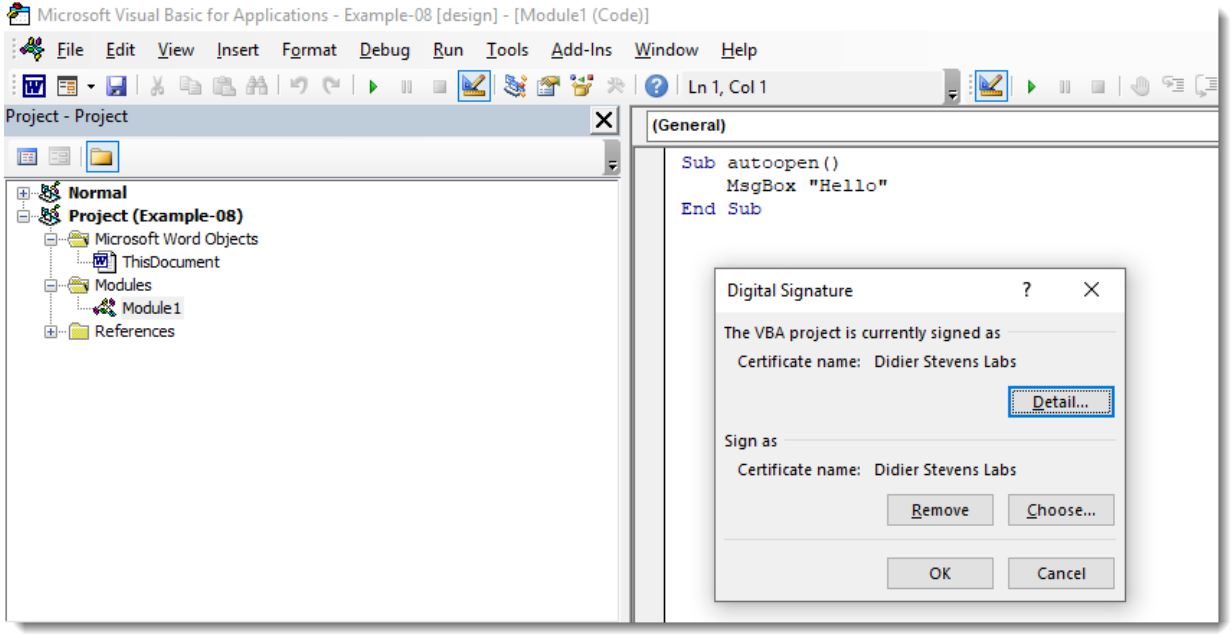
Example 8: Code signing tampering

Tip 4: Abuse!



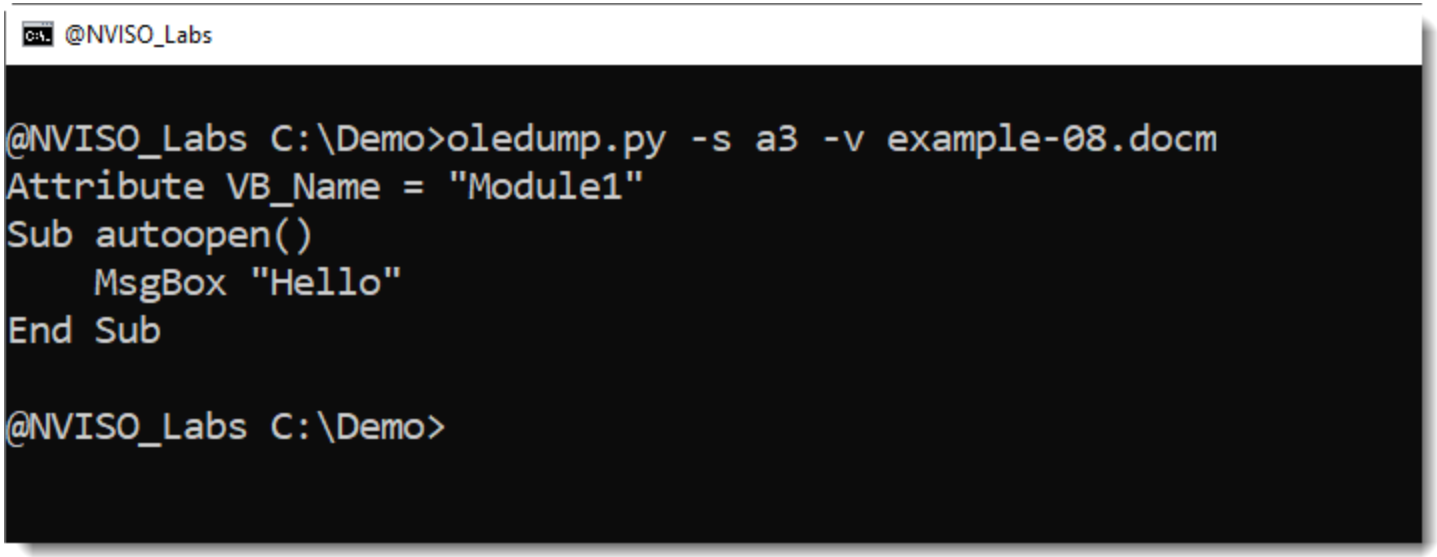
Example 8: Code signing tampering

Tip 4: Abuse!



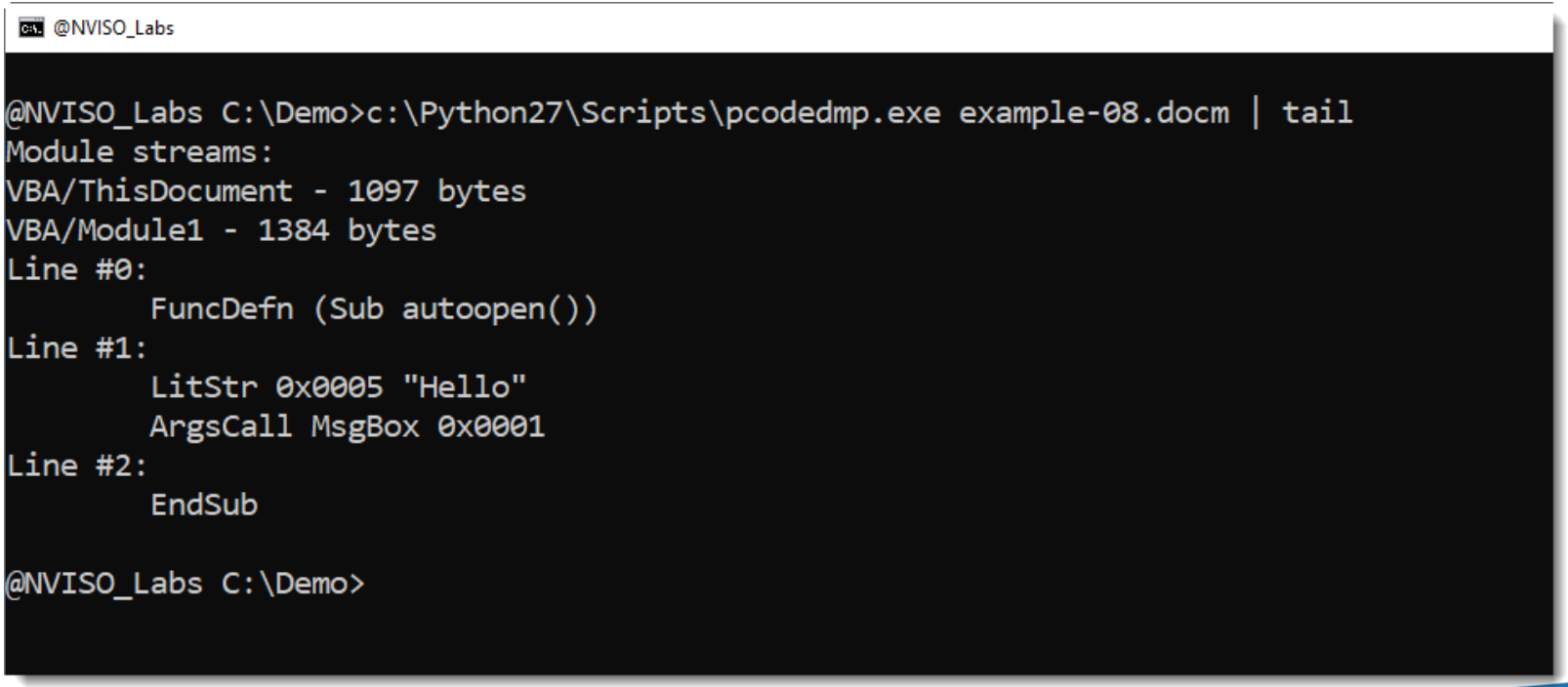
Example 8: Code signing tampering

Tip 4: Abuse!



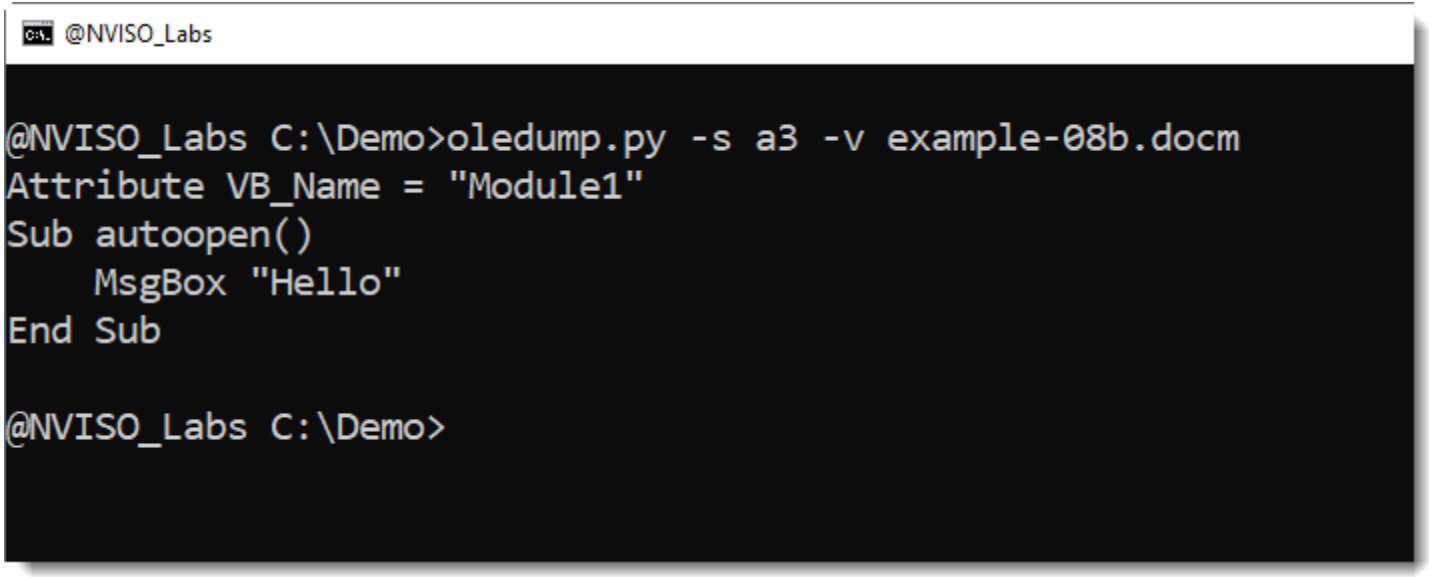
Example 8: Code signing tampering

Tip 4: Abuse!



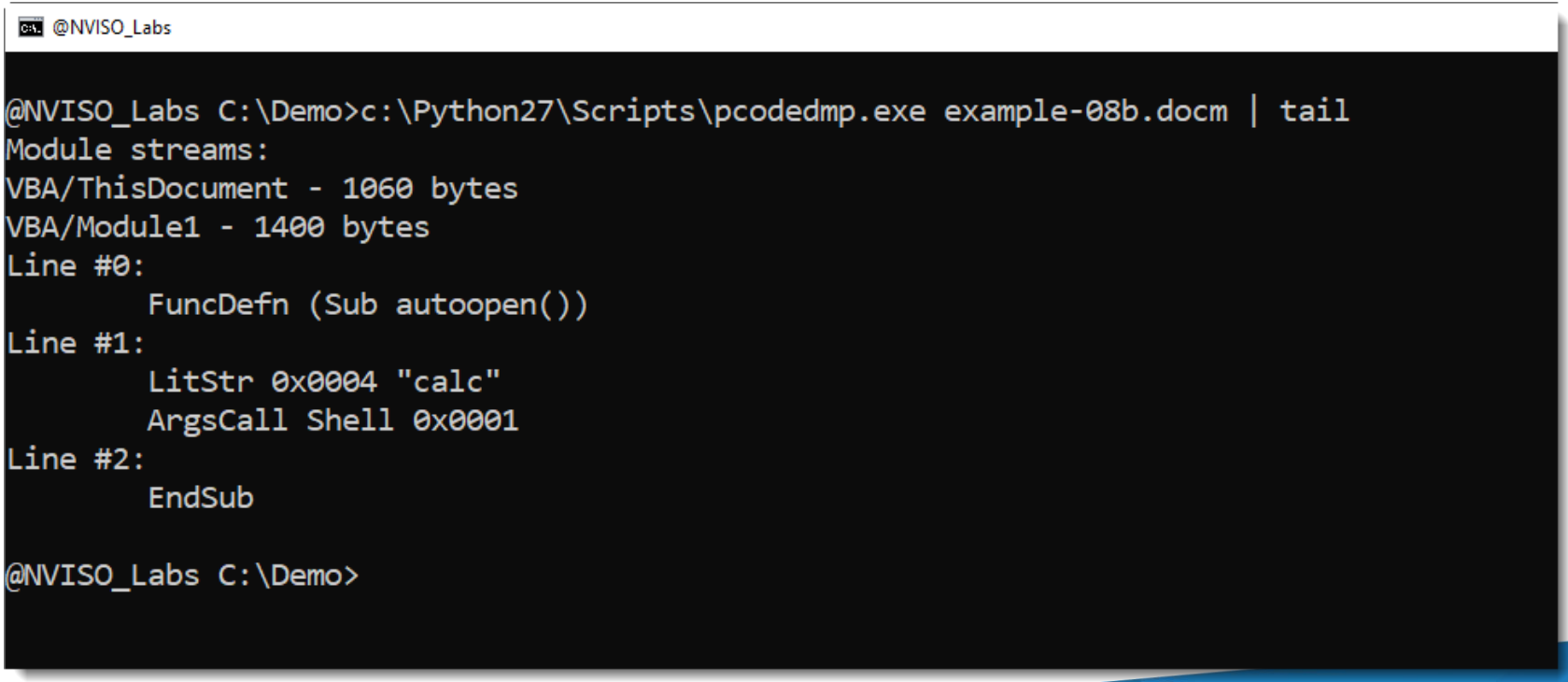
Example 8: Code signing tampering

Tip 4: Abuse!



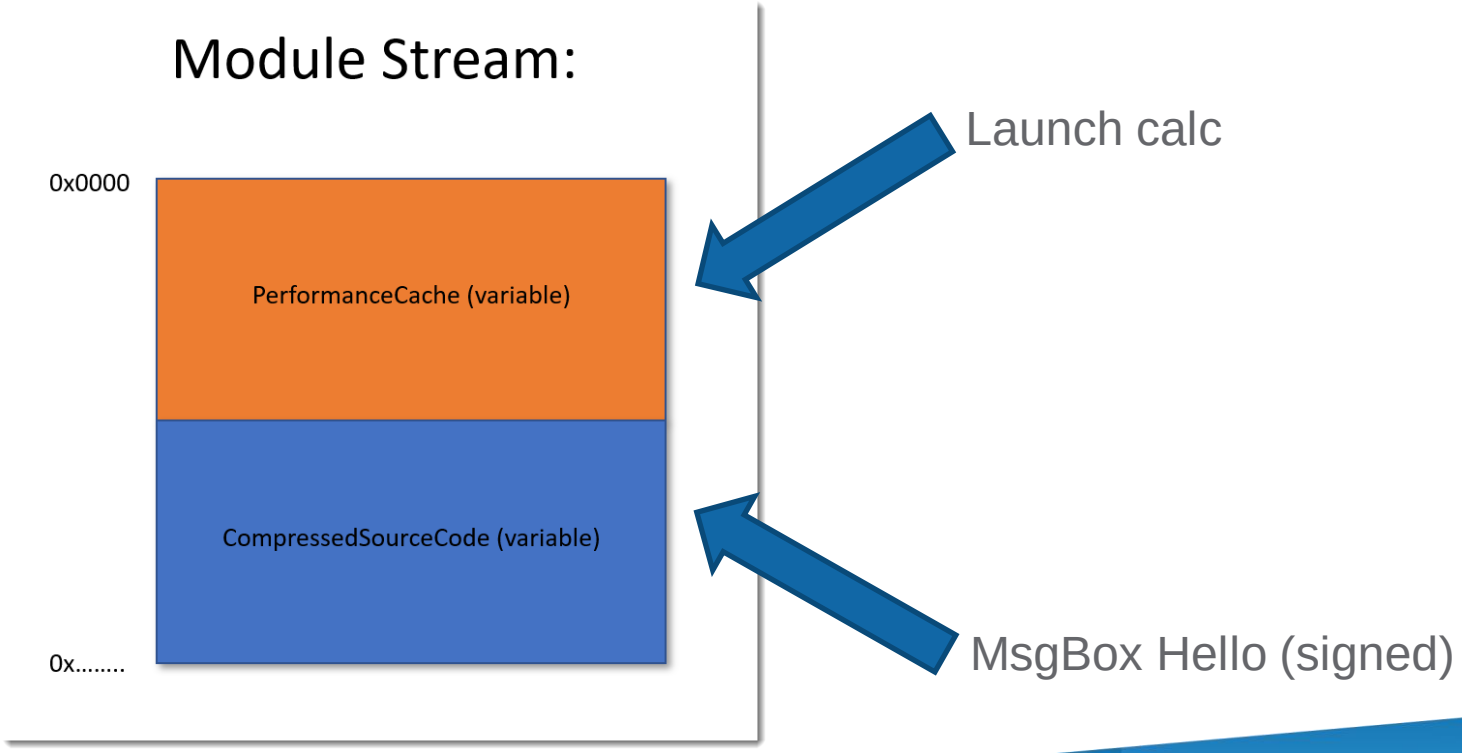
Example 8: Code signing tampering

Tip 4: Abuse!



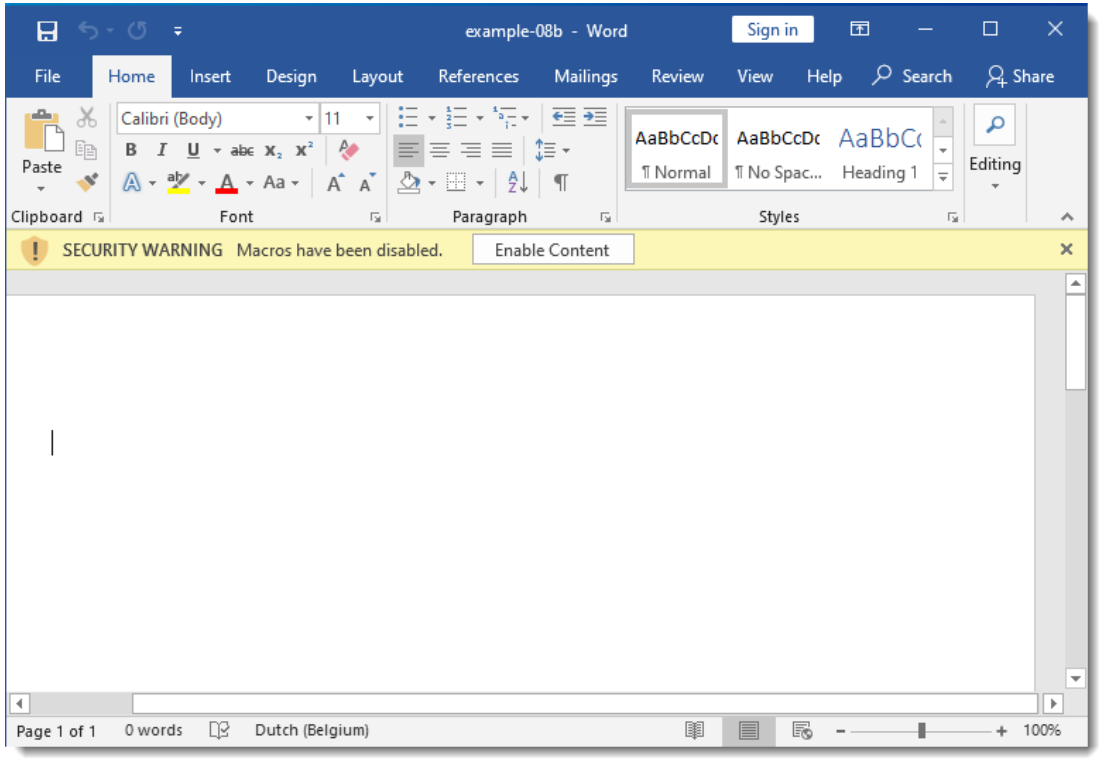
Example 8: Code signing tampering

Tip 4: Abuse!



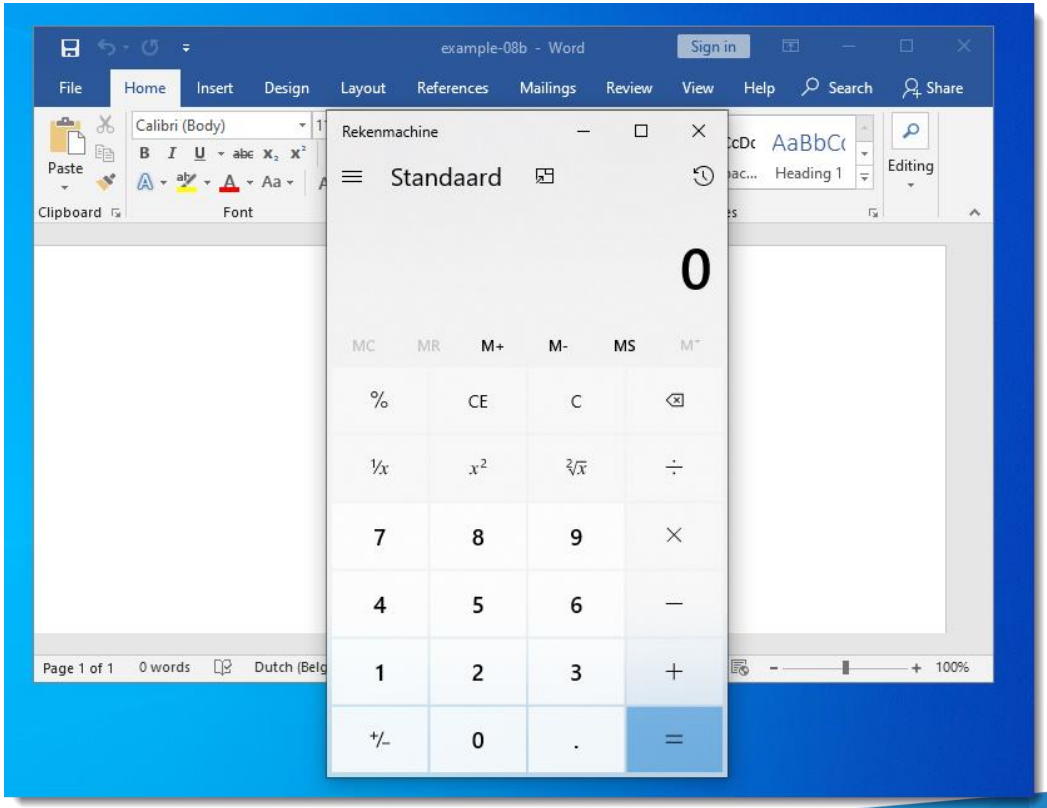
Example 8: Code signing tampering

Tip 4: Abuse!



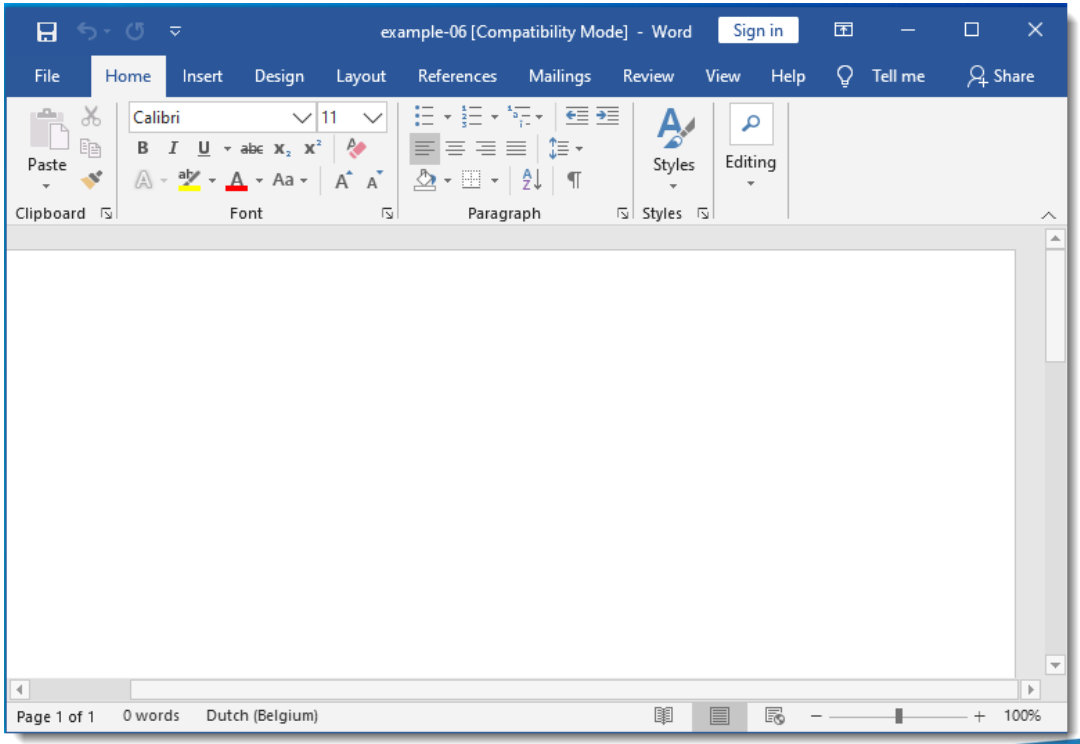
Example 8: Code signing tampering

Tip 4: Abuse!



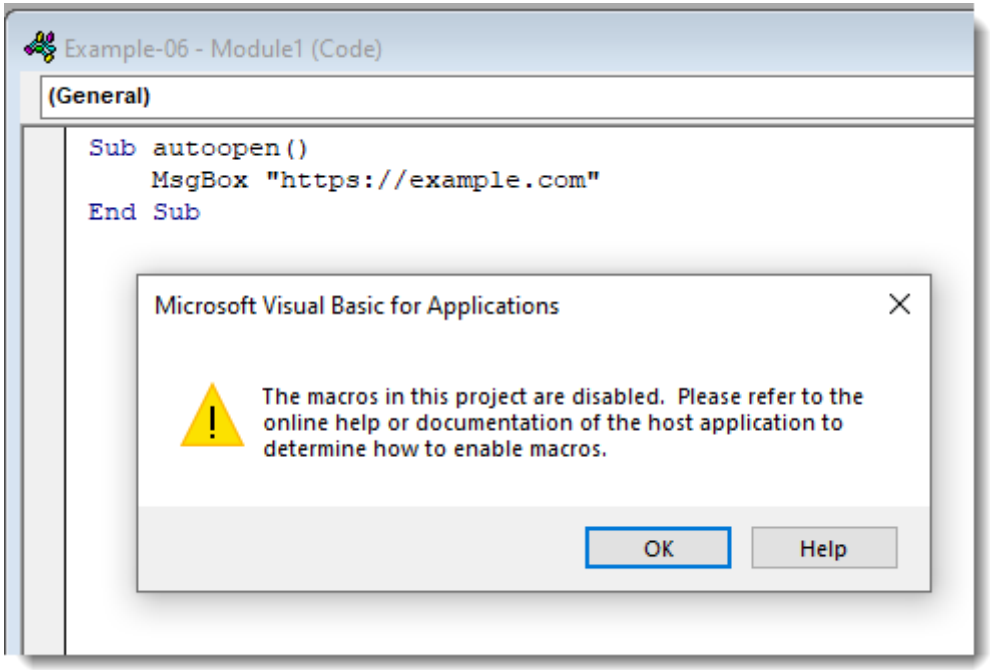
Example 8: Code signing tampering

Tip 4: Abuse!



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)

nviso

4 tips for red teamers

1. Analyze your sh+chr(105)+t
2. Learn from actors
3. RTFM & use it
4. RTFM & abuse it

nviso

More info

https://isc.sans.edu

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

https://blog.nviso.eu

https://blog.didierstevens.com

Questions?

Thank you

www.nviso.eu