www.nviso.eu

Maldocs: a bit of blue, a bit of red

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

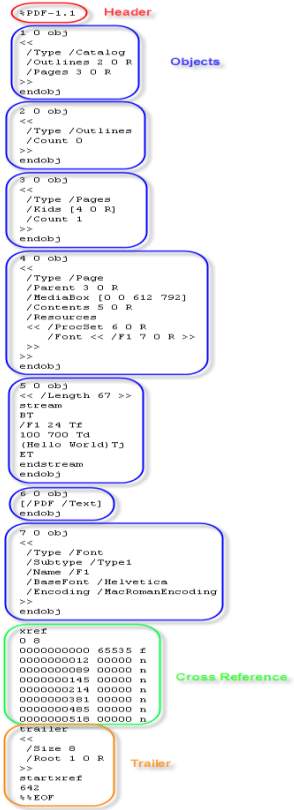
Our Agenda

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

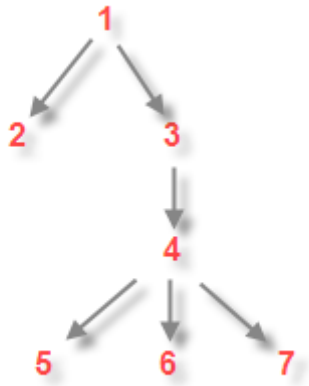
Our Agenda

1 PDF

Maldocs: a bit of blue, a bit of red



Maldocs: a bit of blue, a bit of red



Tracking PDF

(Very similar to phishing PDF)

Demo

https://blog.nviso.eu/2016/11/30/pdf-uris/

Maldocs: a bit of blue, a bit of red

Name Obfuscation

/OpenAction -> /Open#41ction

https://blog.didierstevens.com/2008/04/29/pdf-let-me-count-the-ways/

Maldocs: a bit of blue, a bit of red

Hexadecimal String

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

https://blog.didierstevens.com/2008/04/29/pdf-let-me-count-the-ways/

Maldocs: a bit of blue, a bit of red

nviso

Stream Objects
/ObjStm

https://blog.didierstevens.com/2019/03/07/analyzing-a-phishing-pdf-with-objstm/

QPDF:

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

http://qpdf.sourceforge.net/

My PDF tools:

Analyzing and Creating PDFs

https://blog.didierstevens.com/programs/pdf-tools/

Our Agenda

2 MS Office

Maldocs: a bit of blue, a bit of red

OOXML: Office Open XML

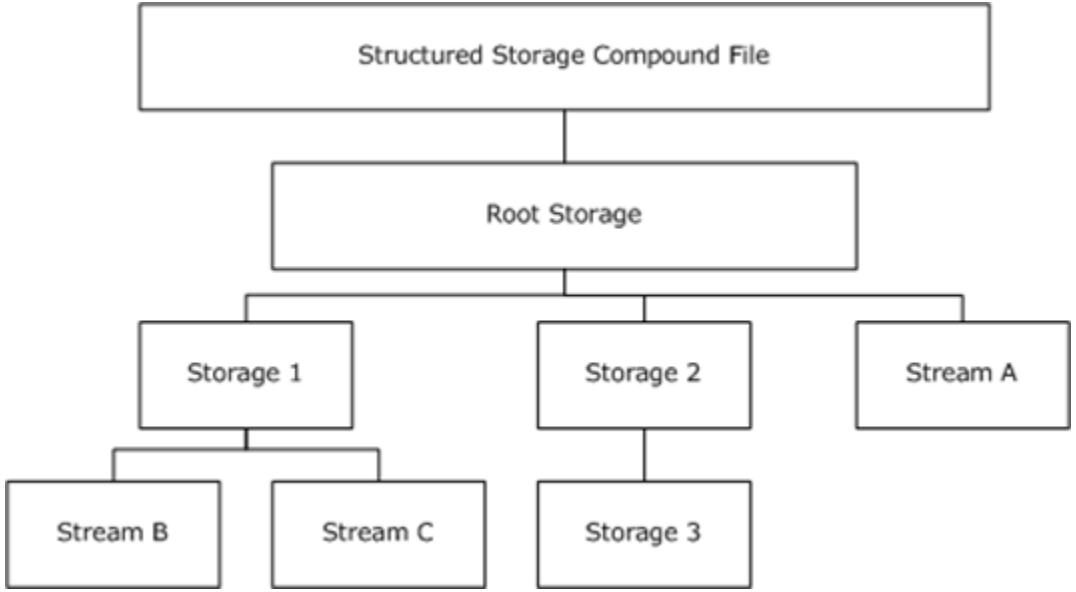
ZIP + XMLs (+ sometimes a bit more)

.docx, .docm, .xlsx, …

CFBF: Compound File Binary Format

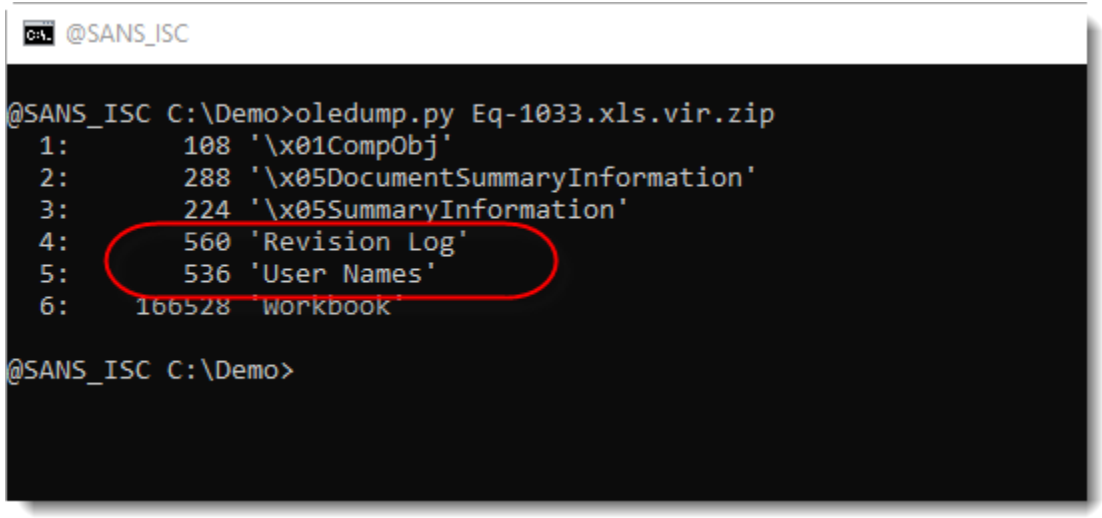
I like to call this OLE format

.doc, .xls, …


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

Demo

Example 1: Zloader Shared Workbook



Example 1: Zloader Shared Workbook

Shared Workbook!

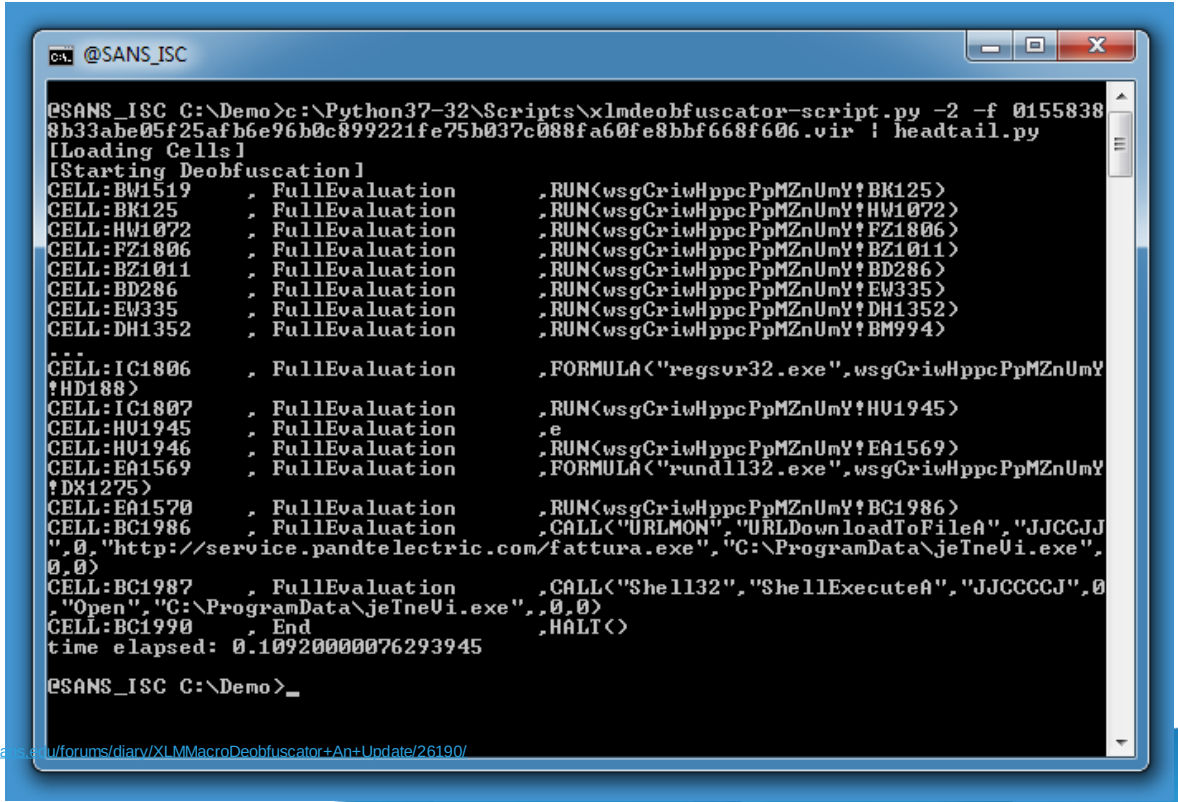
Example 1: Zloader Shared Workbook

YARA Rule:

```
rule zloader_shared_workbook {
    strings:
        $revisionlog = { 52 00 65 00 76 00 69 00 73 00 69 00 6F 00 6E 00 20 00 4C 00 6F 00 67 00 00 00 00 00 00 00 00 00 }
        $usernames = { 55 00 73 00 65 00 72 00 20 00 4E 00 61 00 6D 00 65 00 73 00 00 00 00 00 00 00 00 00 00 00 00 00 }
        $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 }
    condition:
        $revisionlog and $usernames and $workbook and uint32be(0) == 0xd0cf11e0
}
```

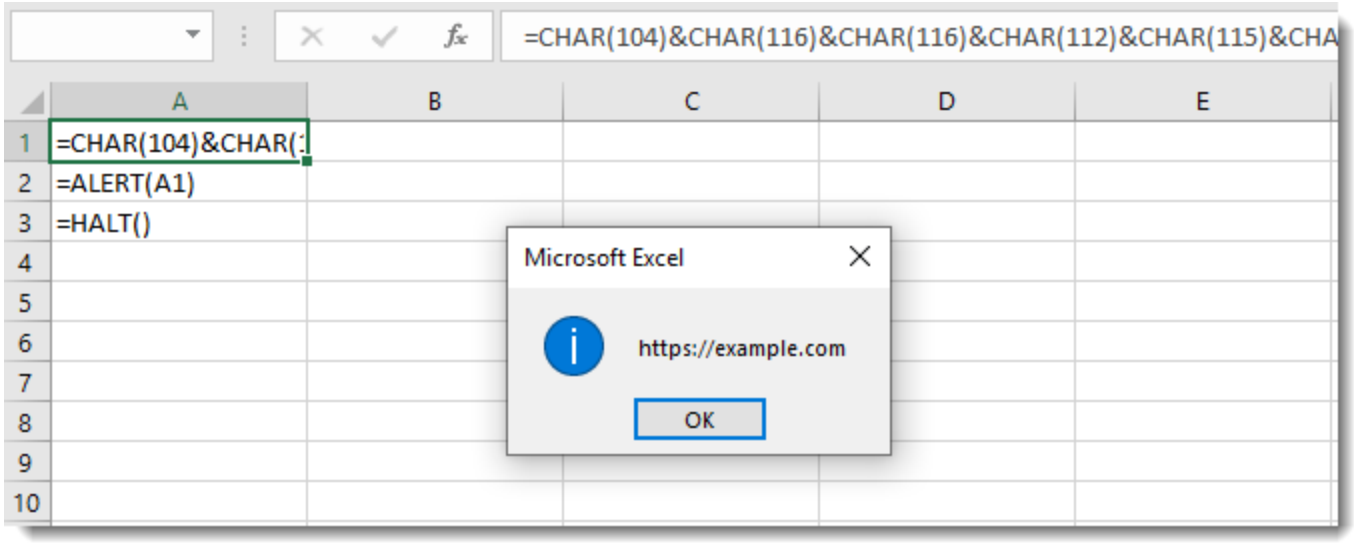
Example 1: Zloader Shared Workbook

XLMMacroDeobfuscator

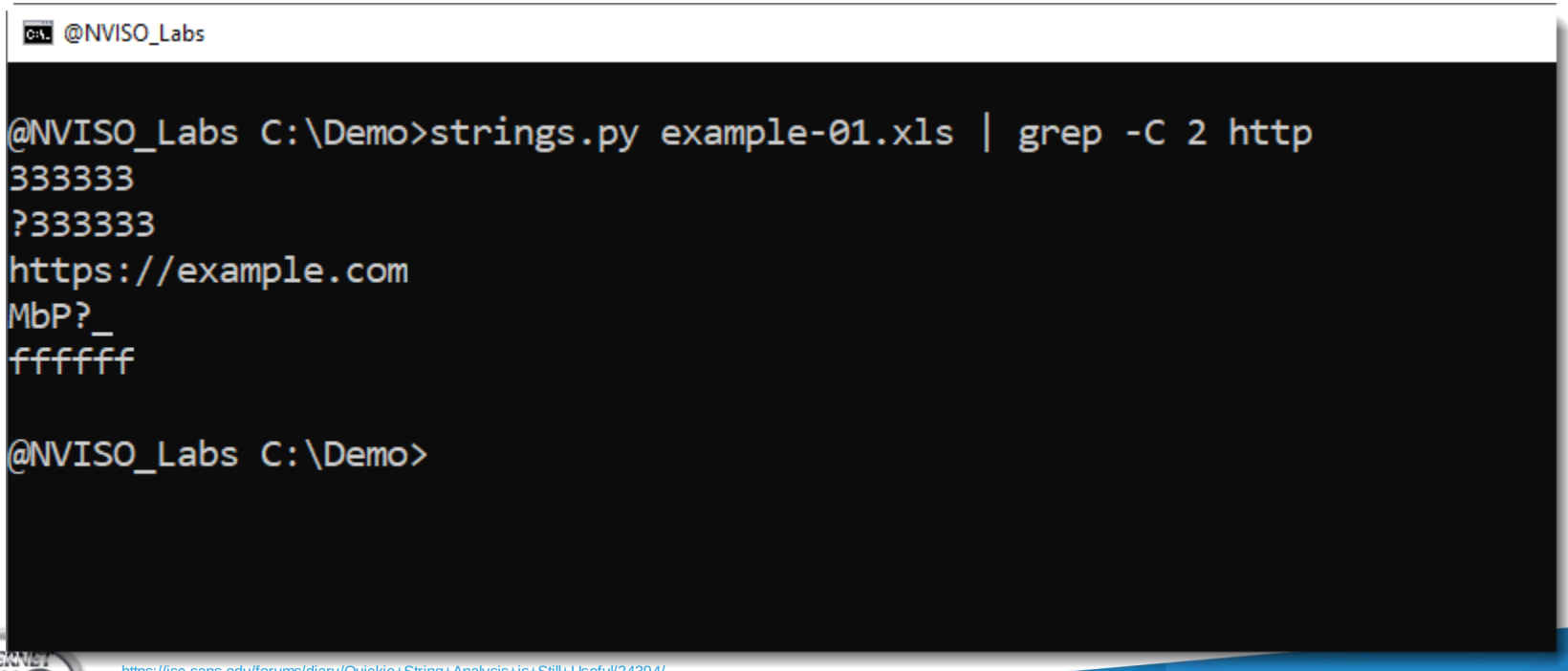


https://isc.sans.edu/forums/diary/XLMMacroDeobfuscator+An+Update/26190/

Example 2: the power of strings

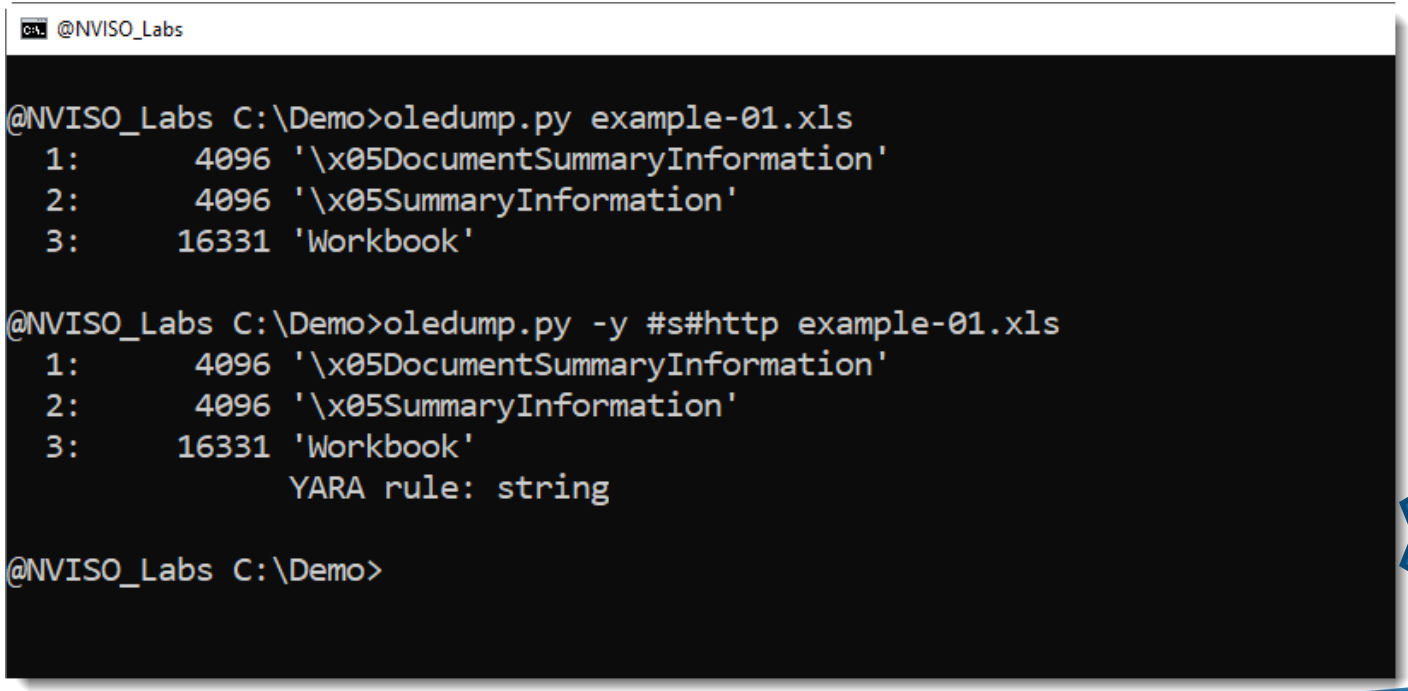


Example 2: the power of strings



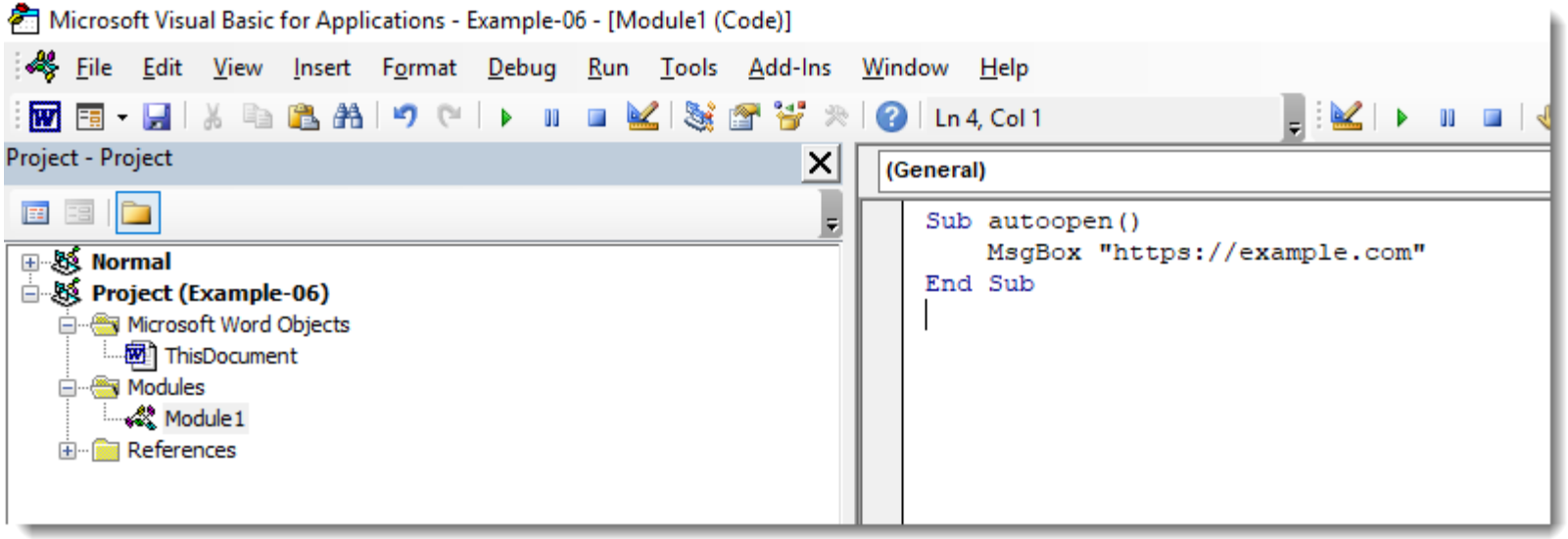
https://isc.sans.edu/forums/diary/Quickie+String+Analysis+is+Still+Useful/24394/

Example 2: the power of strings

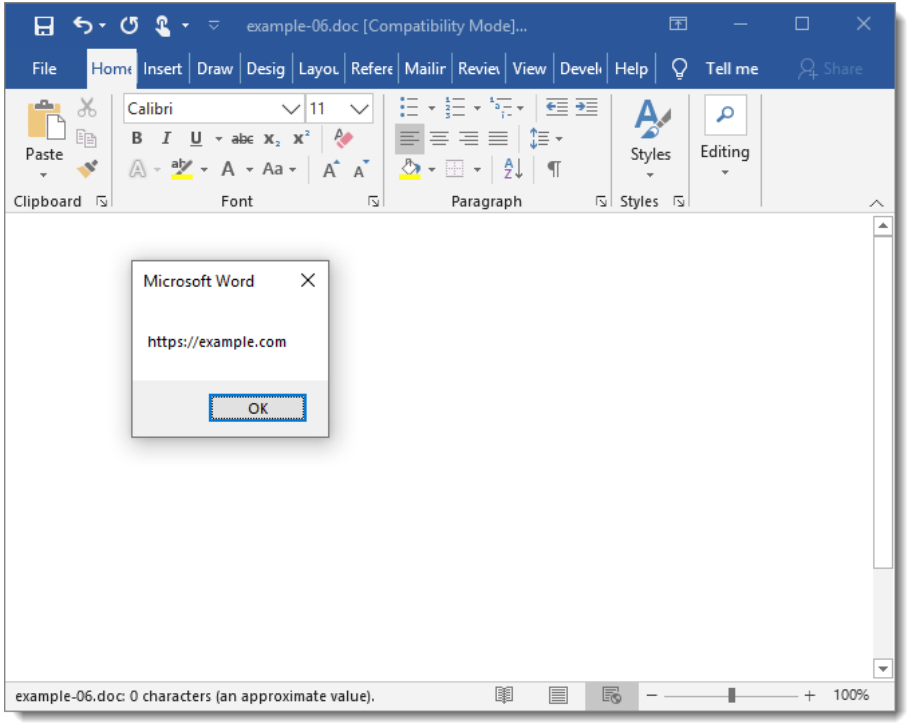


Demo

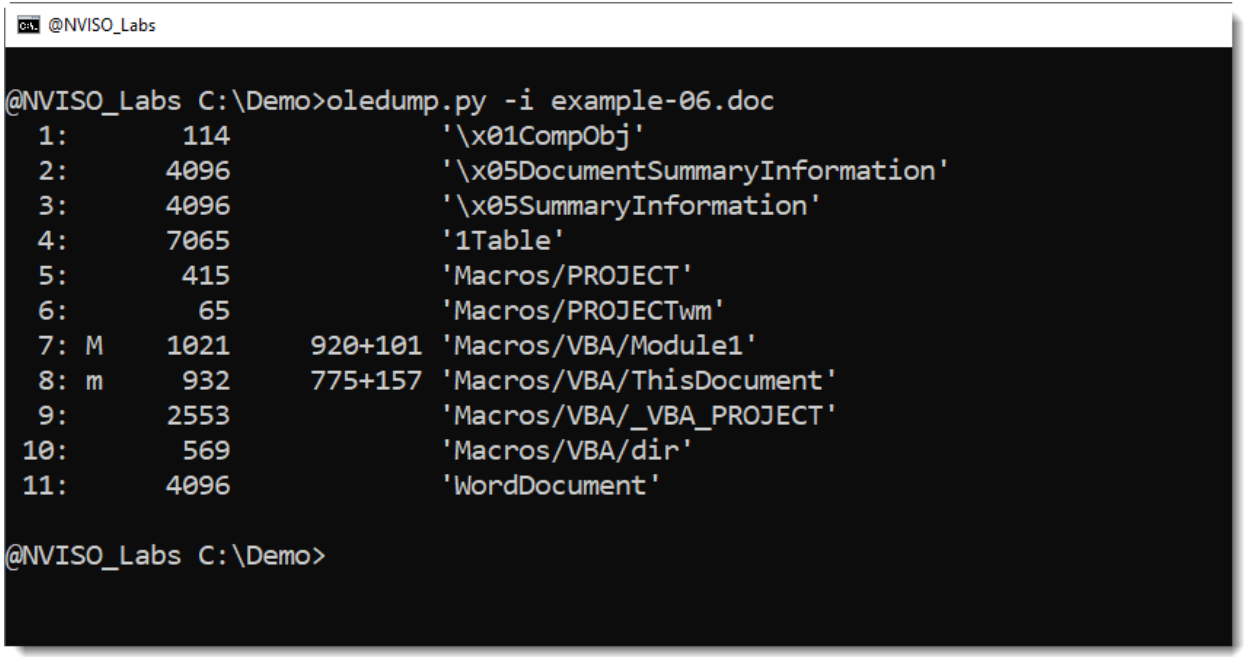
Example 3: VBA stomping



Example 3: VBA stomping



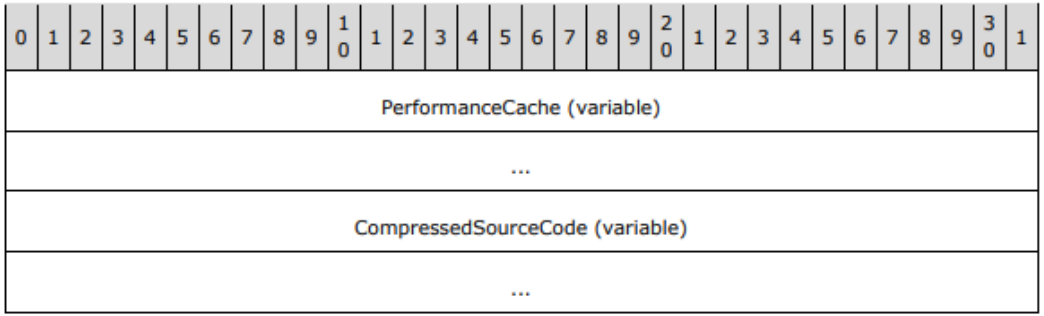
Example 3: VBA stomping



Example 3: VBA stomping

2.3.4.3 Module Stream: Visual Basic Modules

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



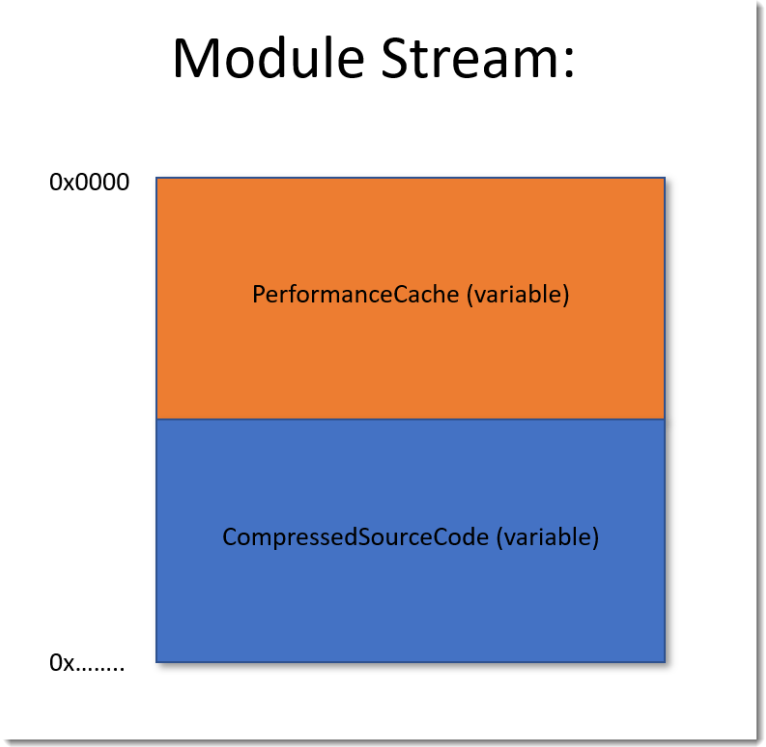
0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
PerformanceCache (variable)																															
...																															
CompressedSourceCode (variable)																															
...																															

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.

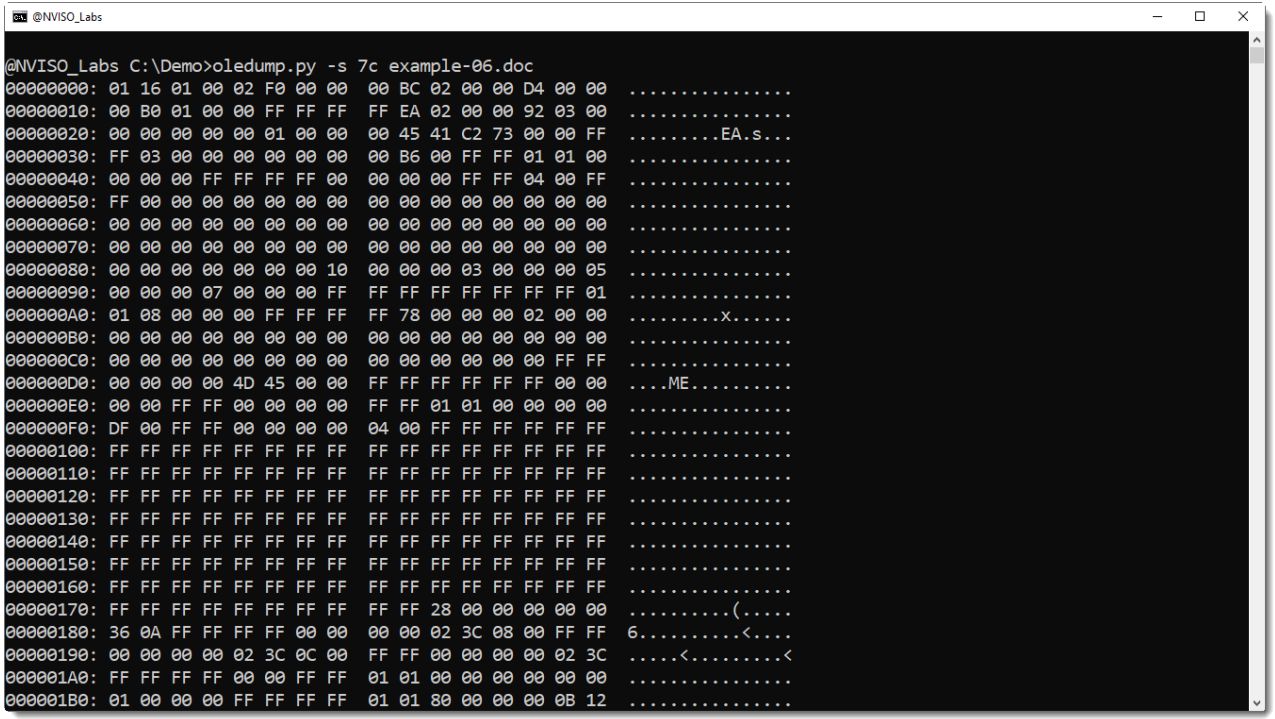
CompressedSourceCode (variable): An array of bytes compressed as specified in Compression (section 2.4.1). When decompressed yields an array of bytes that specifies the textual representation of **VBA** language source code as specified in [MS-VBAL] section 4.2. MUST contain **MBCS** characters encoded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

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

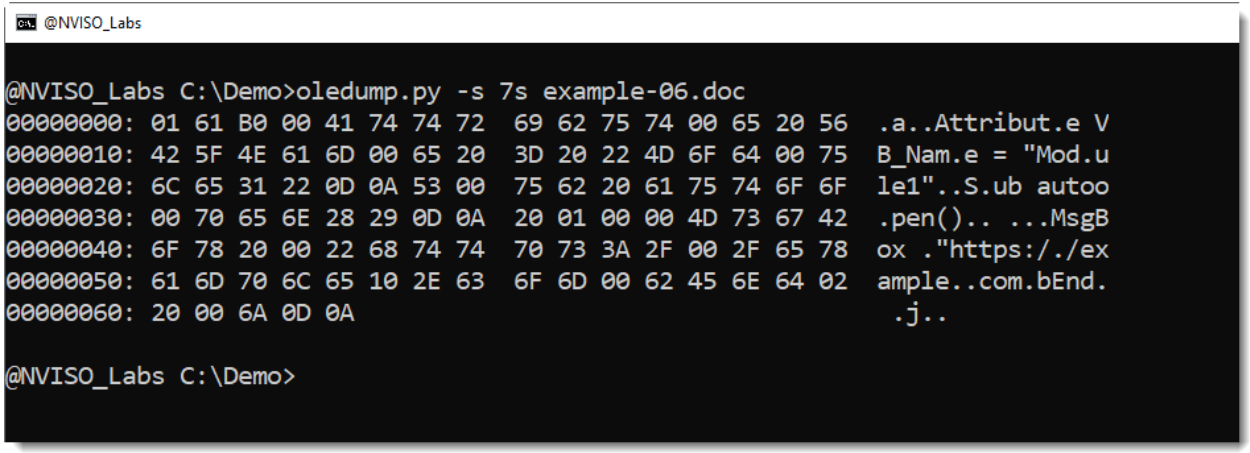
Example 3: VBA stomping



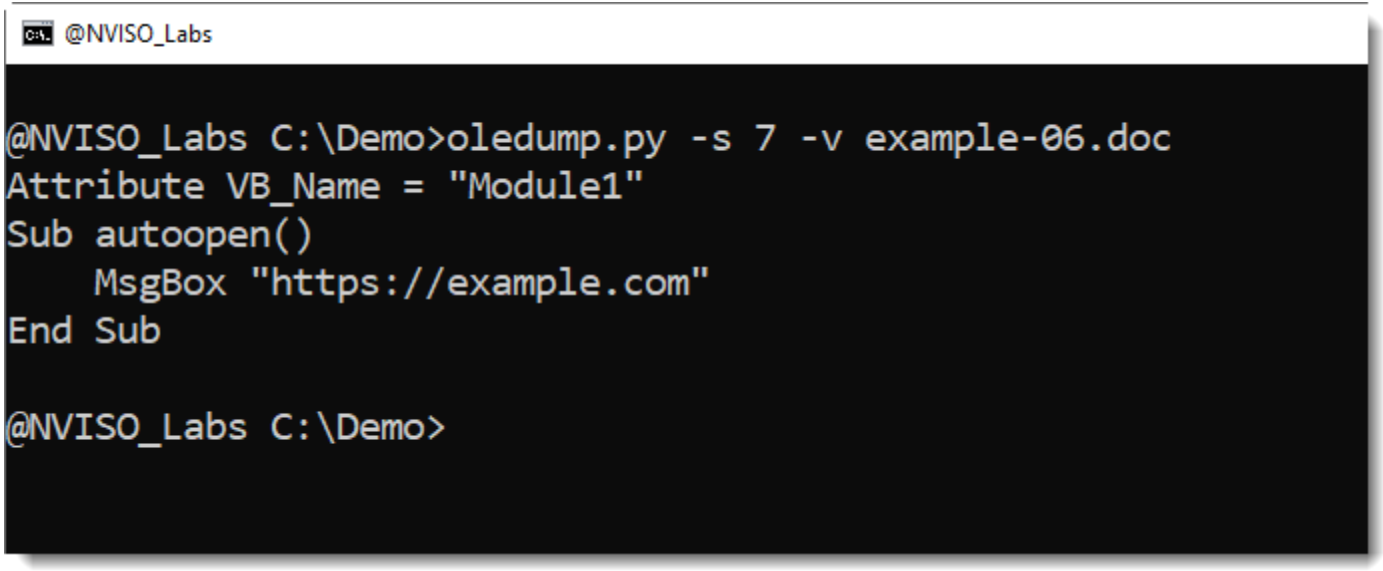
Example 3: VBA stomping



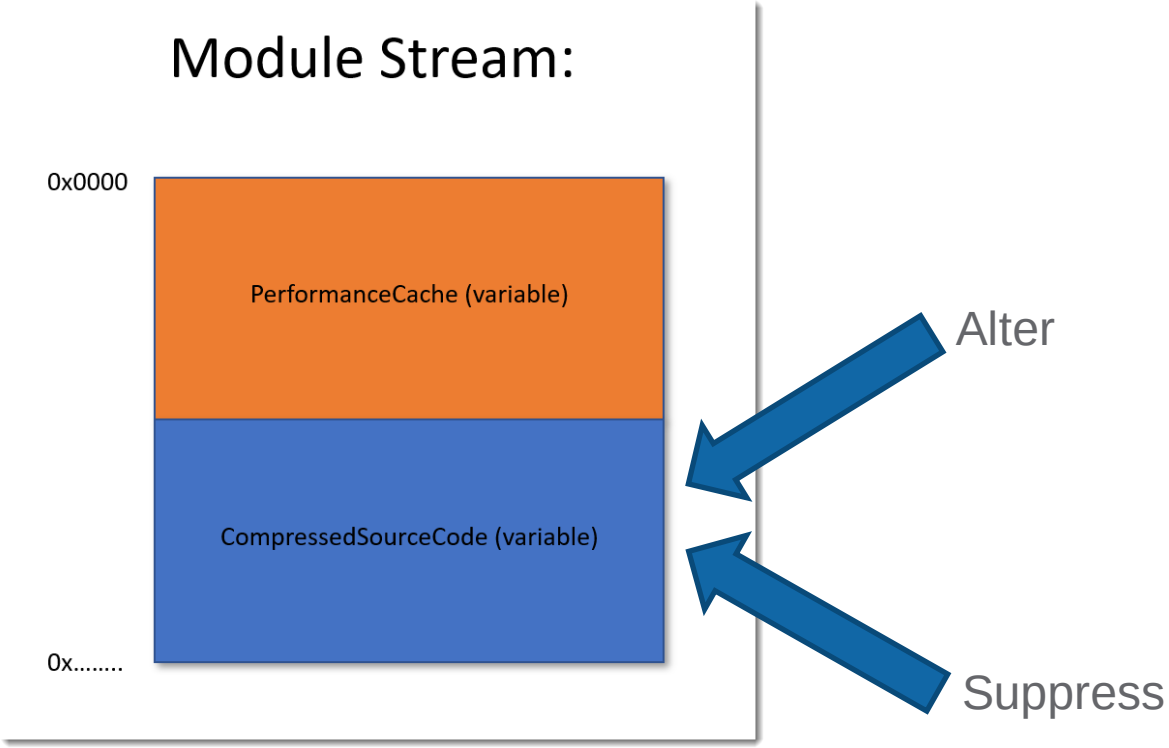
Example 3: VBA stomping



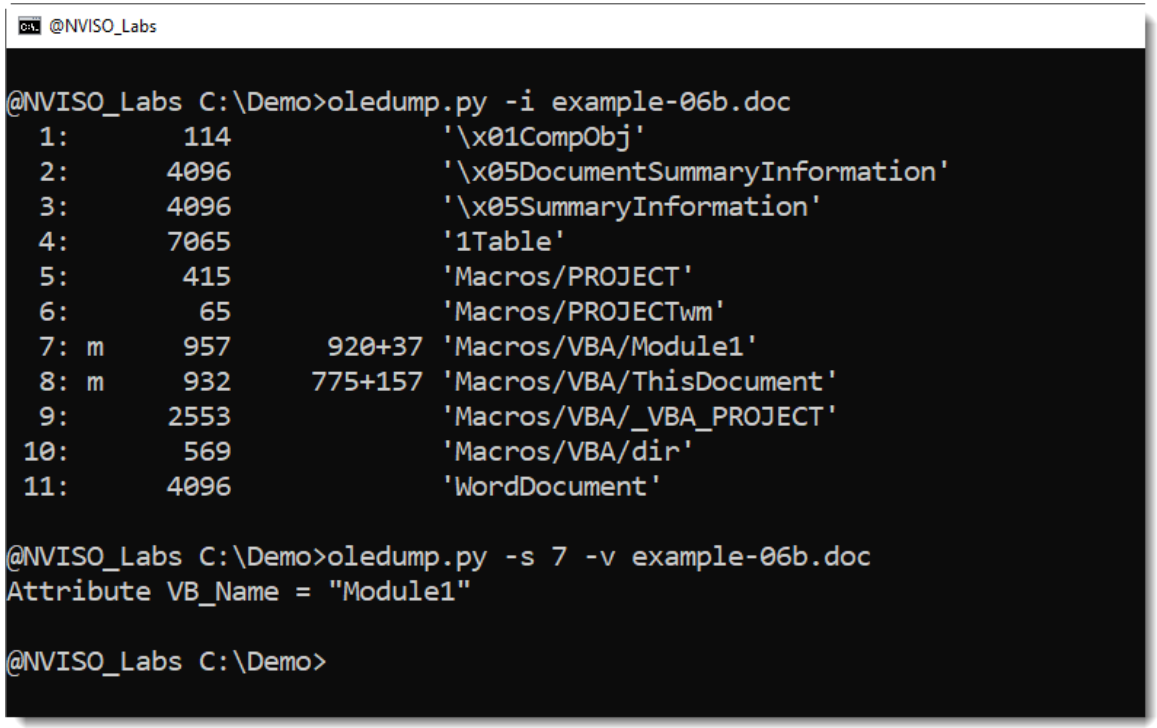
Example 3: VBA stomping



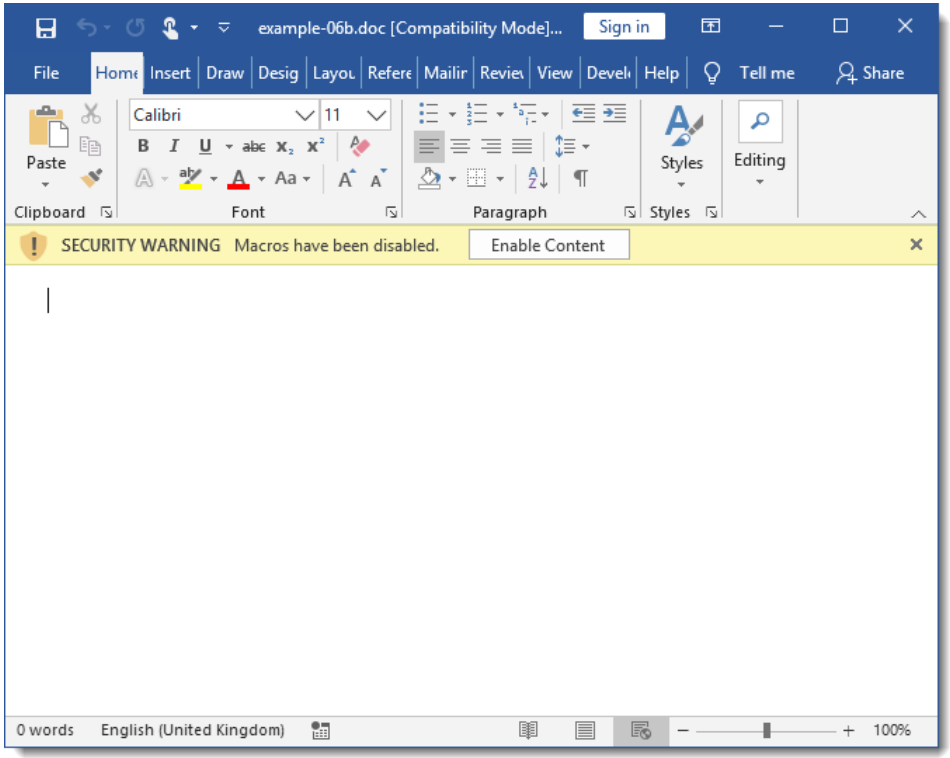
Example 3: VBA stomping



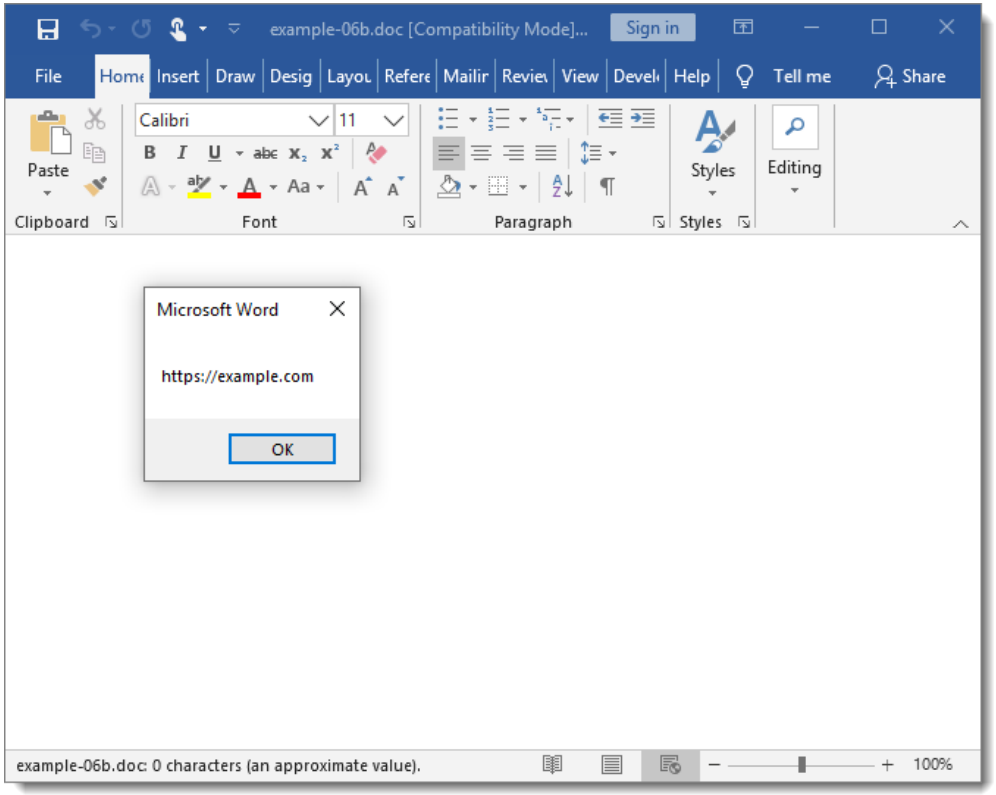
Example 3: VBA stomping



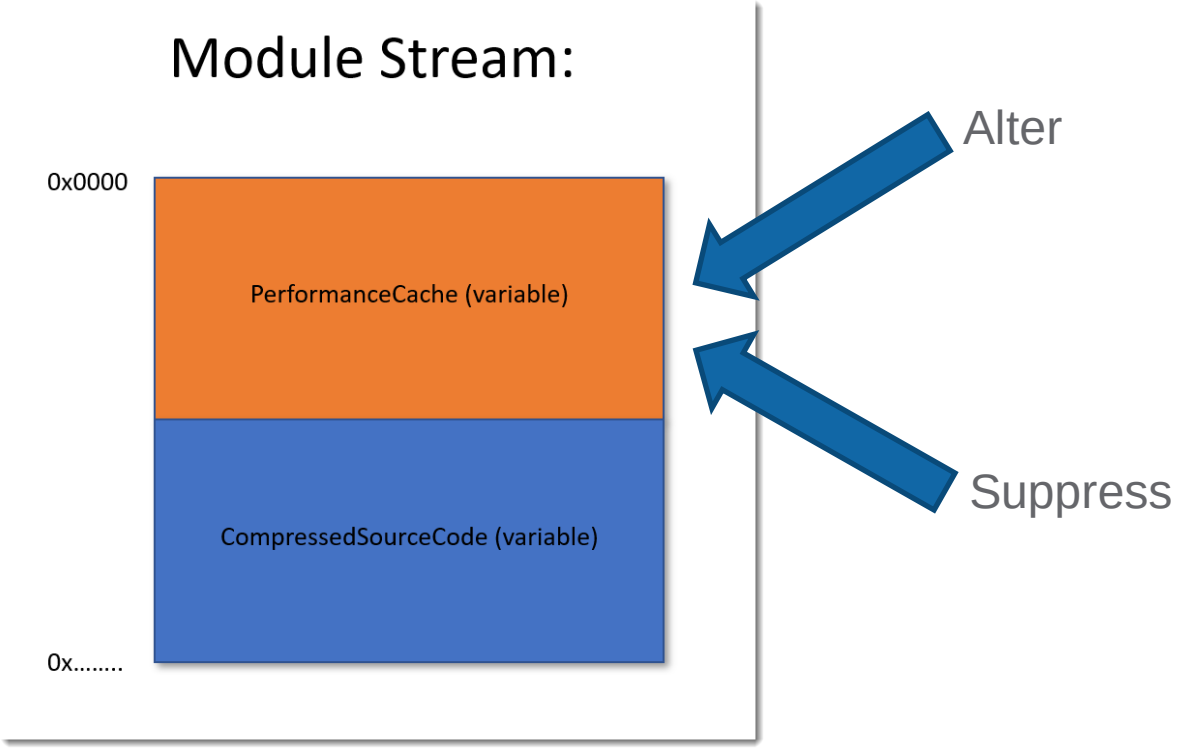
Example 3: VBA stomping



Example 3: VBA stomping

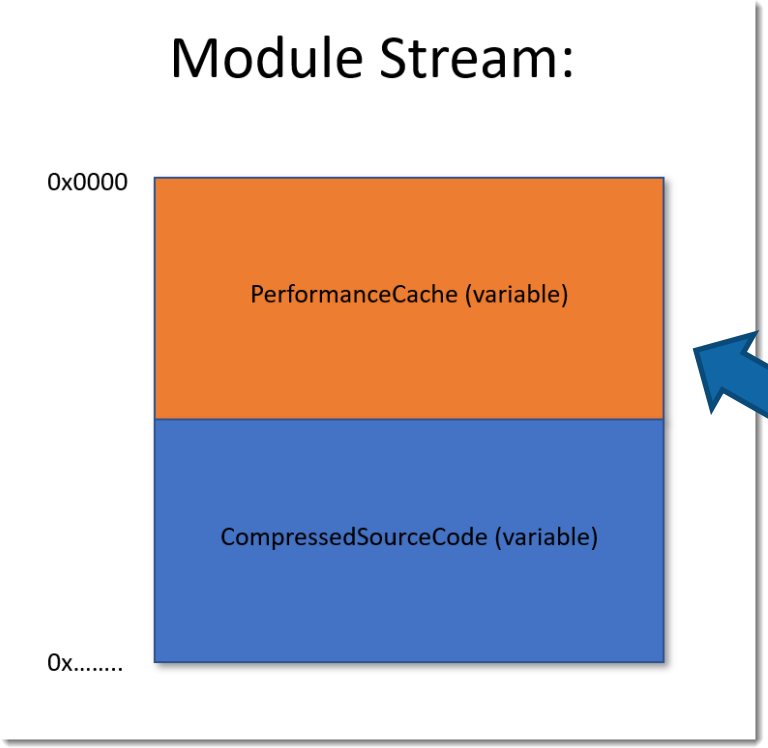


Example 4: VBA purging



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

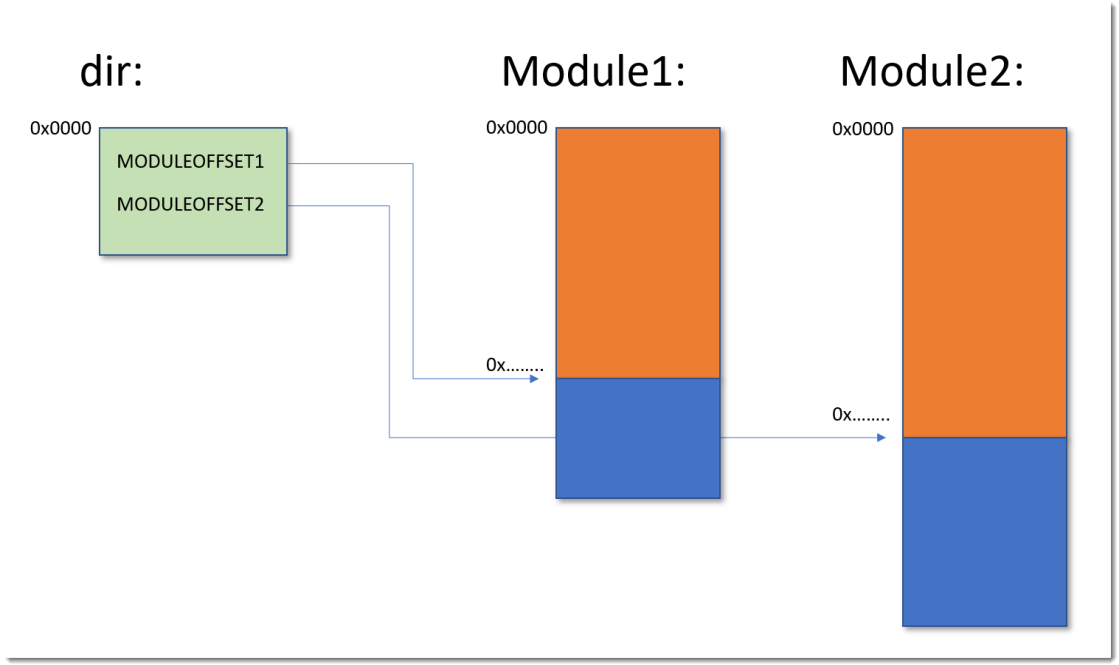
Example 4: VBA purging



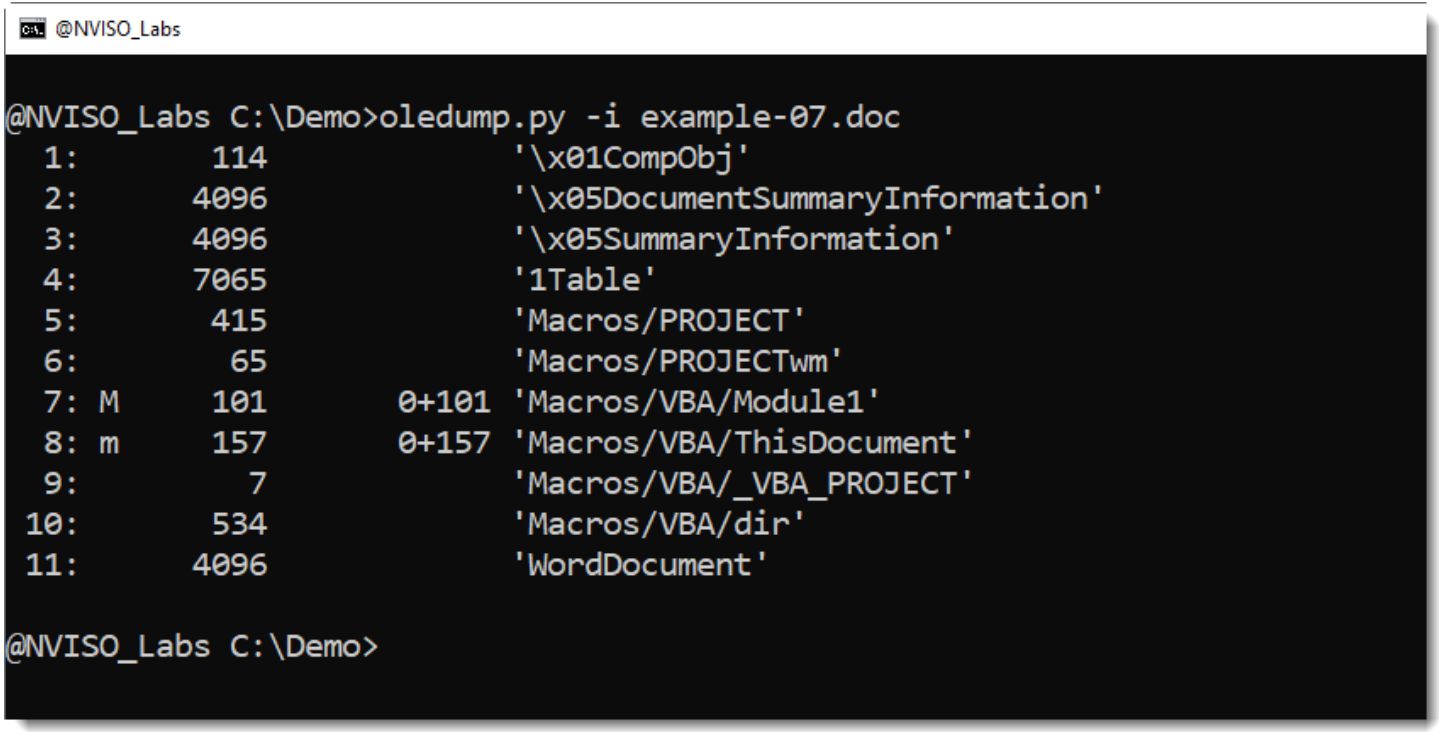
Suppress -> VBA Purging

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

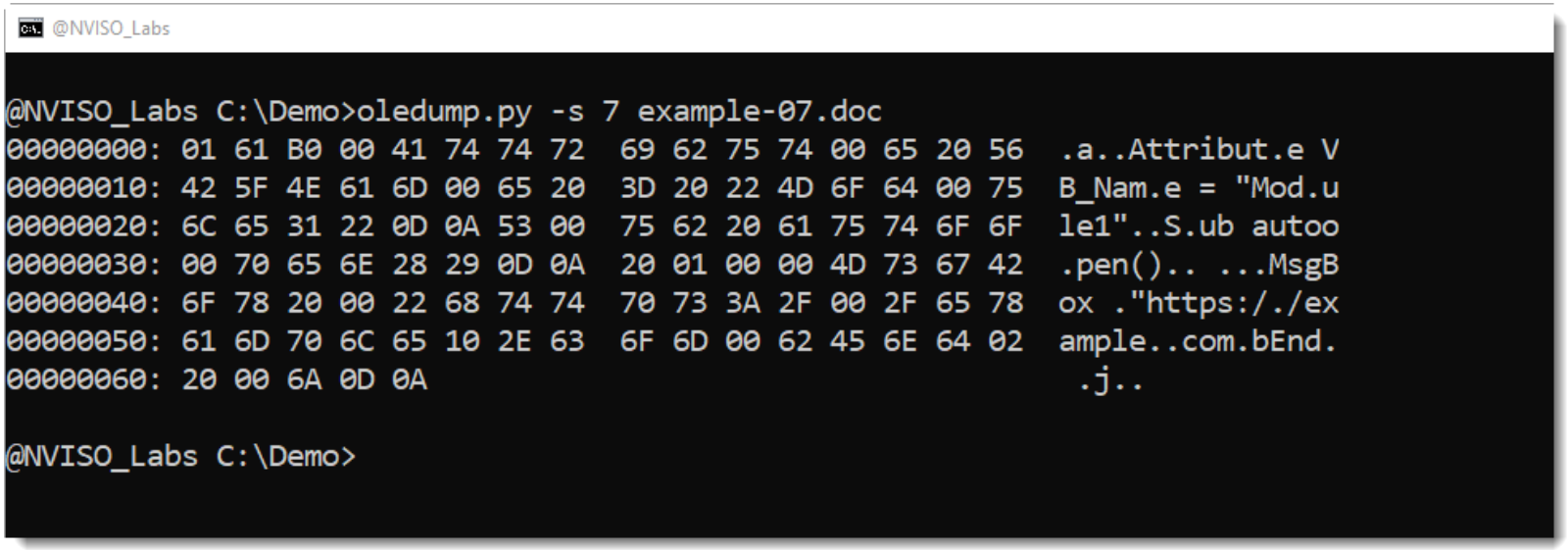
Example 4: VBA purging



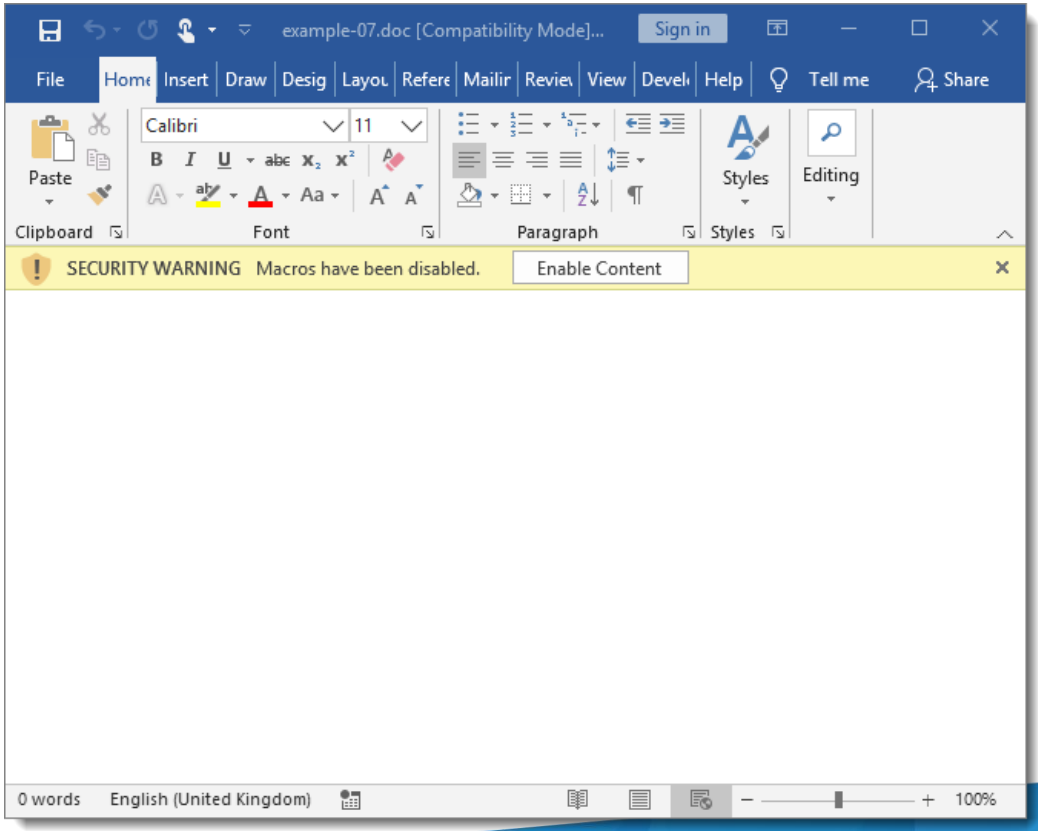
Example 4: VBA purging



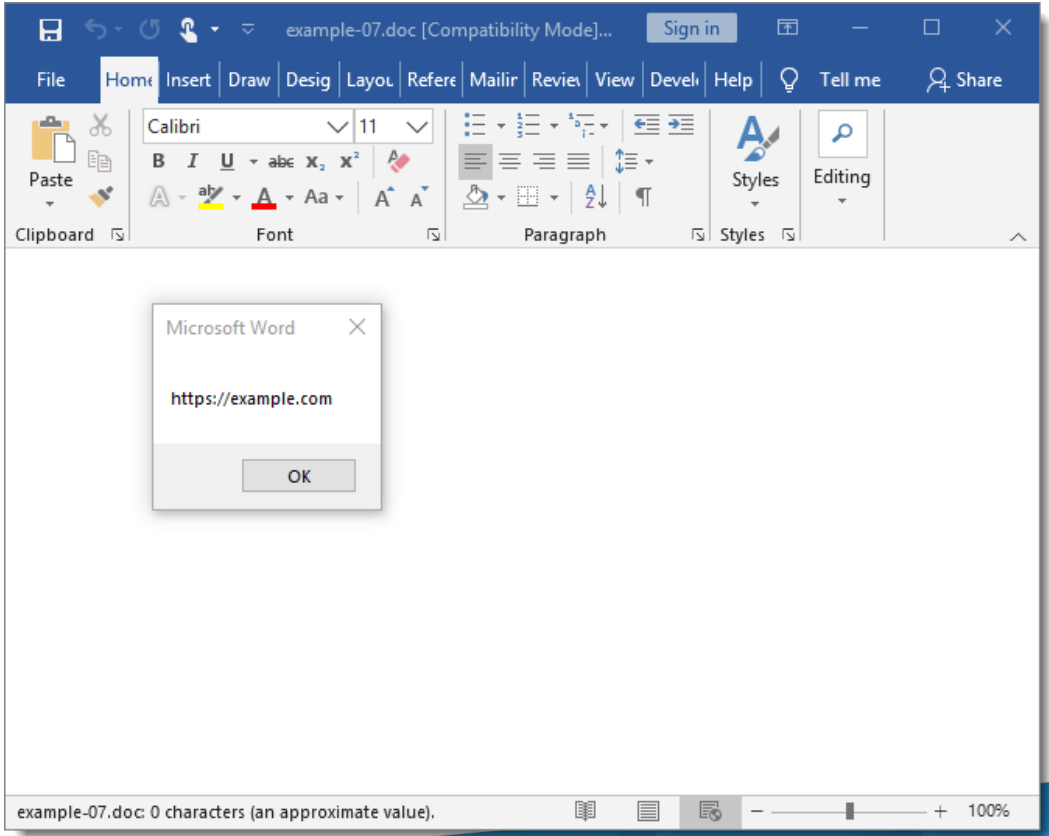
Example 4: VBA purging



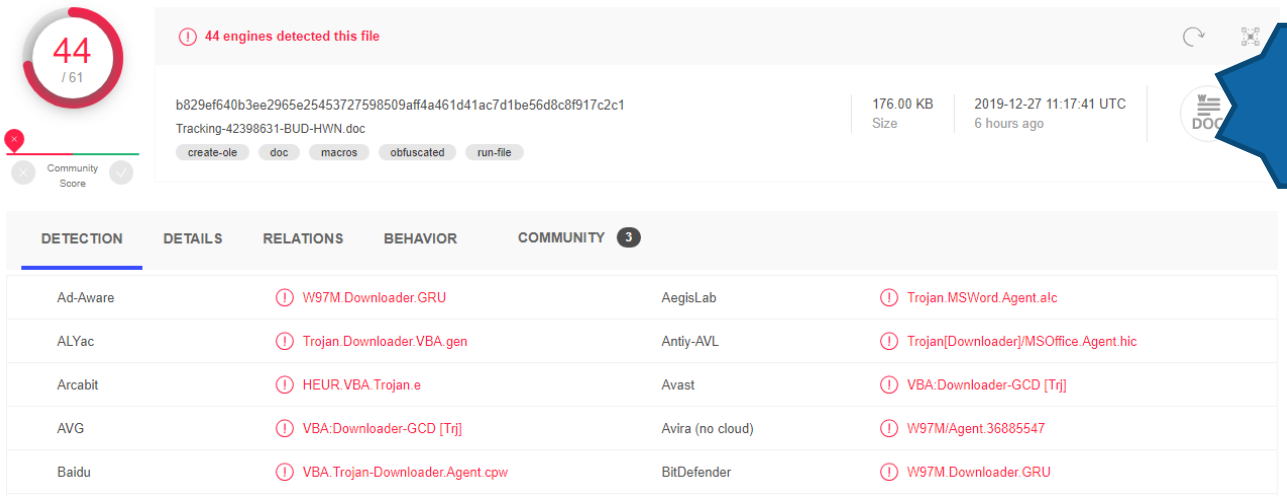
Example 4: VBA purging



Example 4: VBA purging

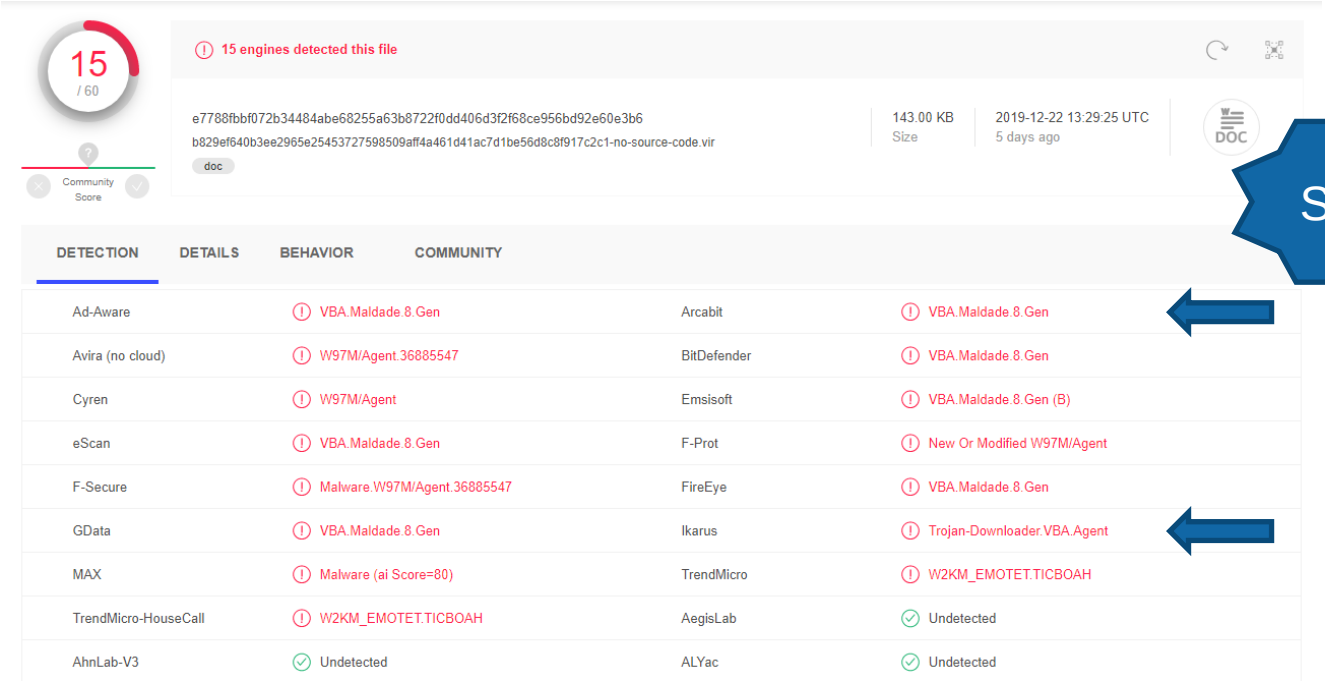


Example 4: VBA purging



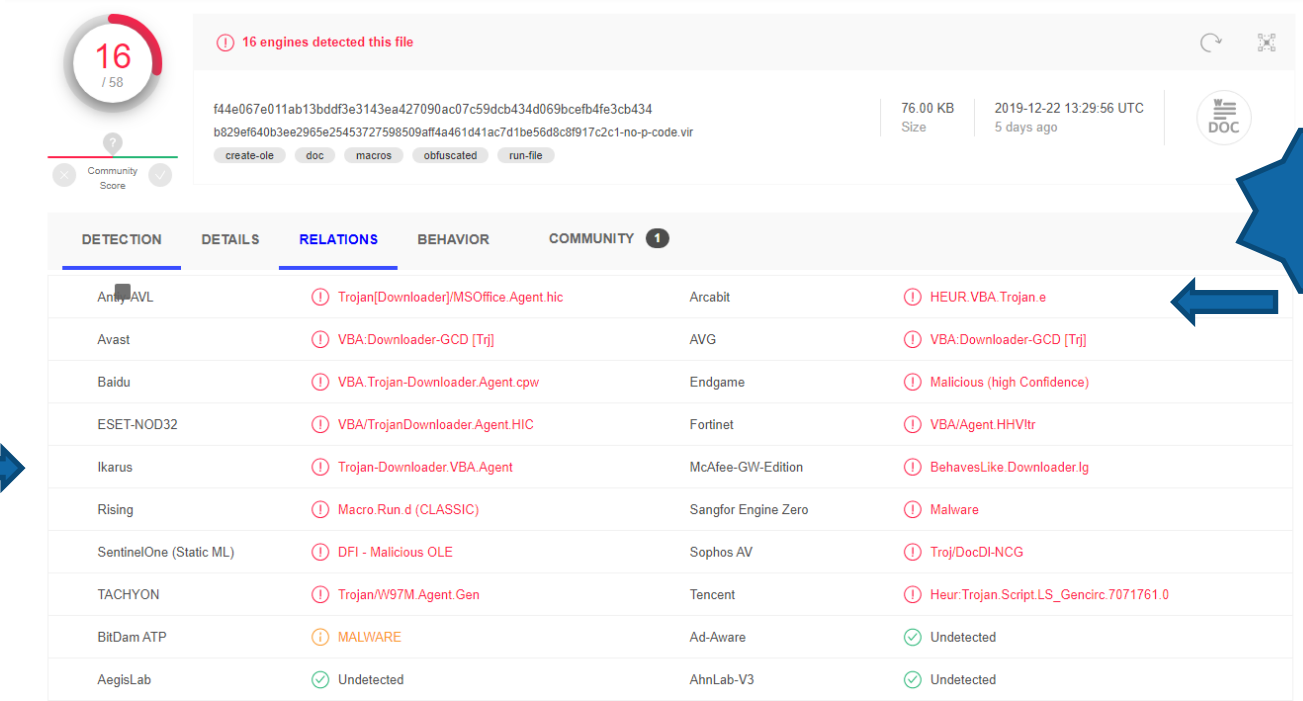
https://www.virustotal.com/gui/file/b829ef640b3ee2965e25453727598509aff4a461d41ac7d1be56d8c8f917c2c1/detection

Example 4: VBA purging



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

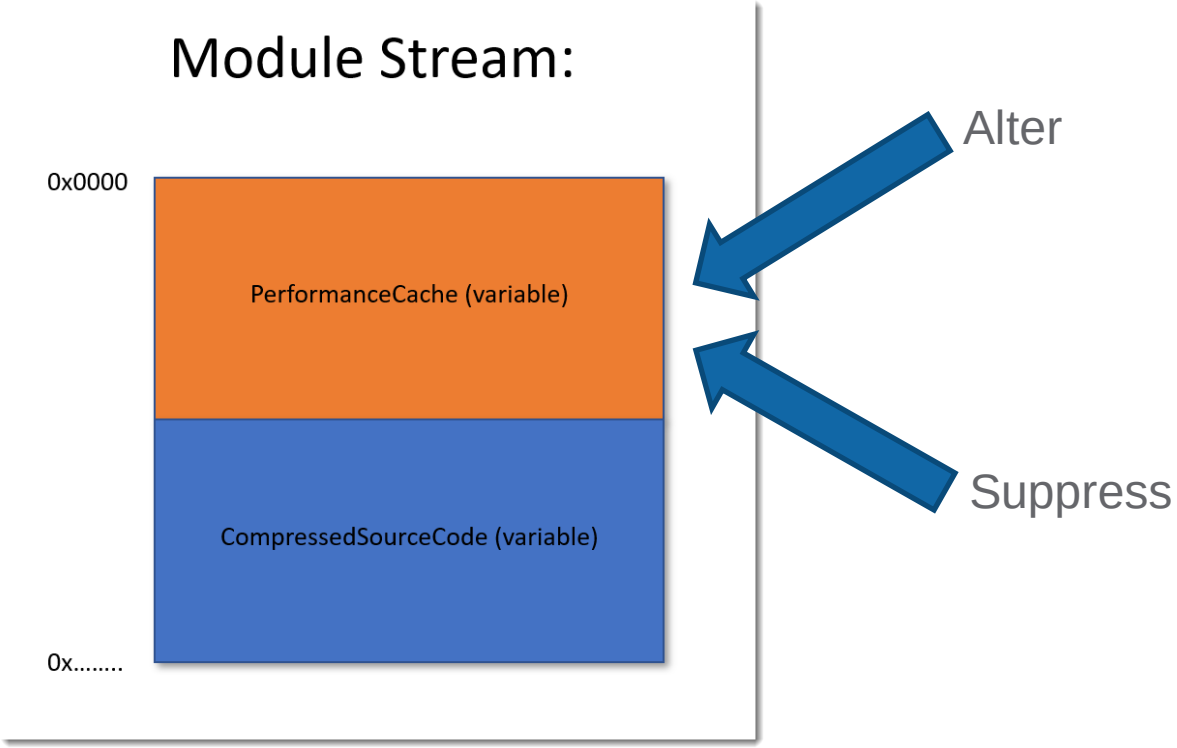
Example 4: VBA purging



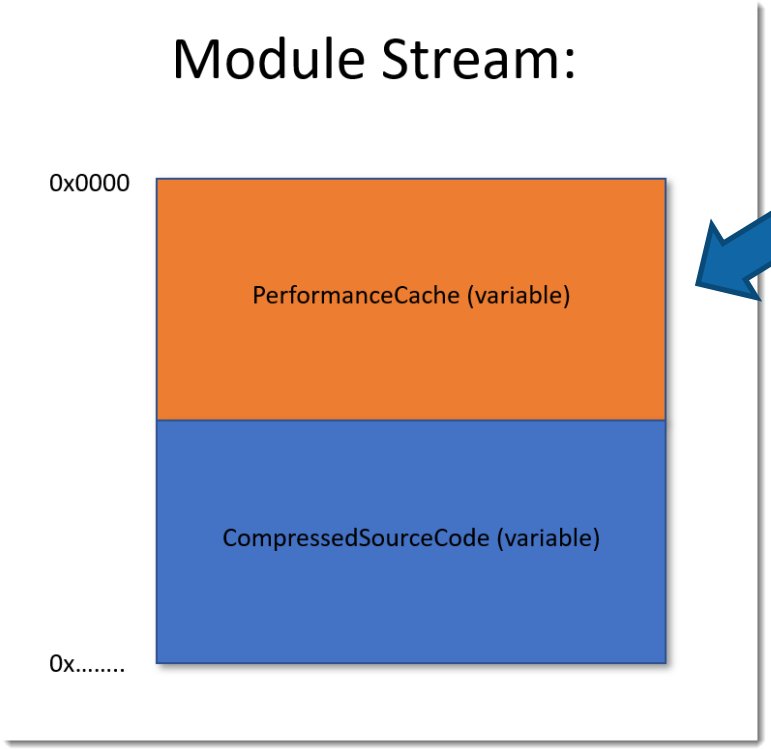
Purged

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

Example 5: Code signing tampering



Example 5: Code signing tampering



Alter -> code signing tampering

https://blog.nviso.eu/2020/06/04/tampering-with-digitally-signed-vba-projects/

Example 5: 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.

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

Example 5: Code signing tampering

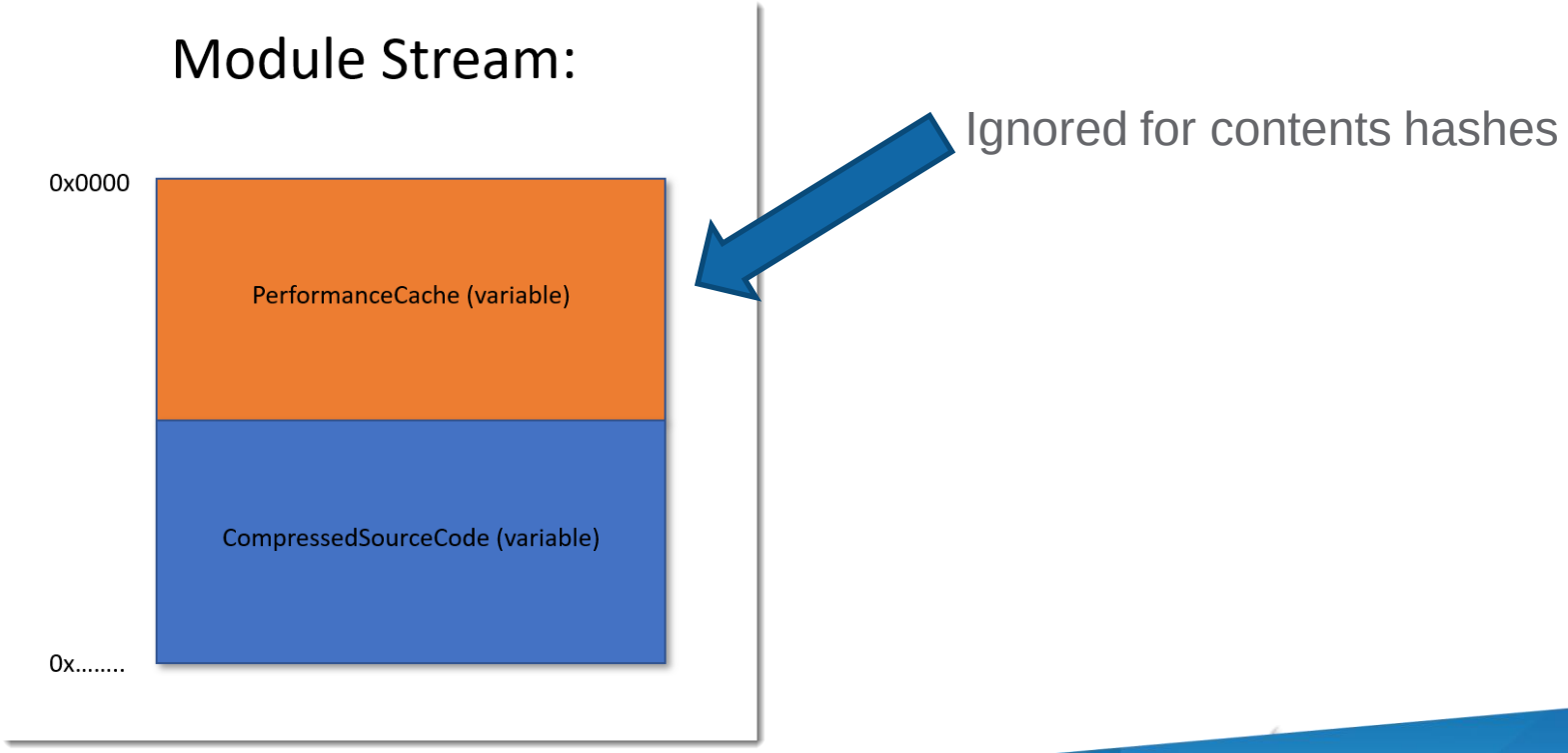
```
FOR EACH ModuleStream (section 2.3.4.3) IN VBA Storage (section 2.3.4) of Storage

   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
```


[MS-OVBA] - v20200219
Office VBA File Format Structure

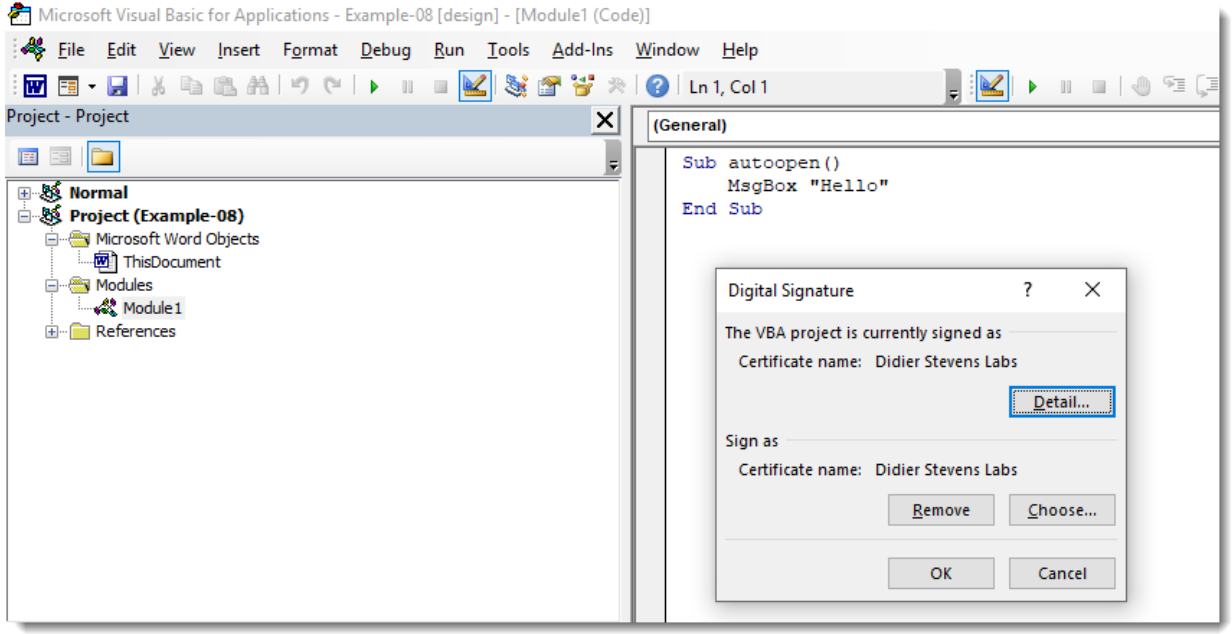
Release: February 19, 2020

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

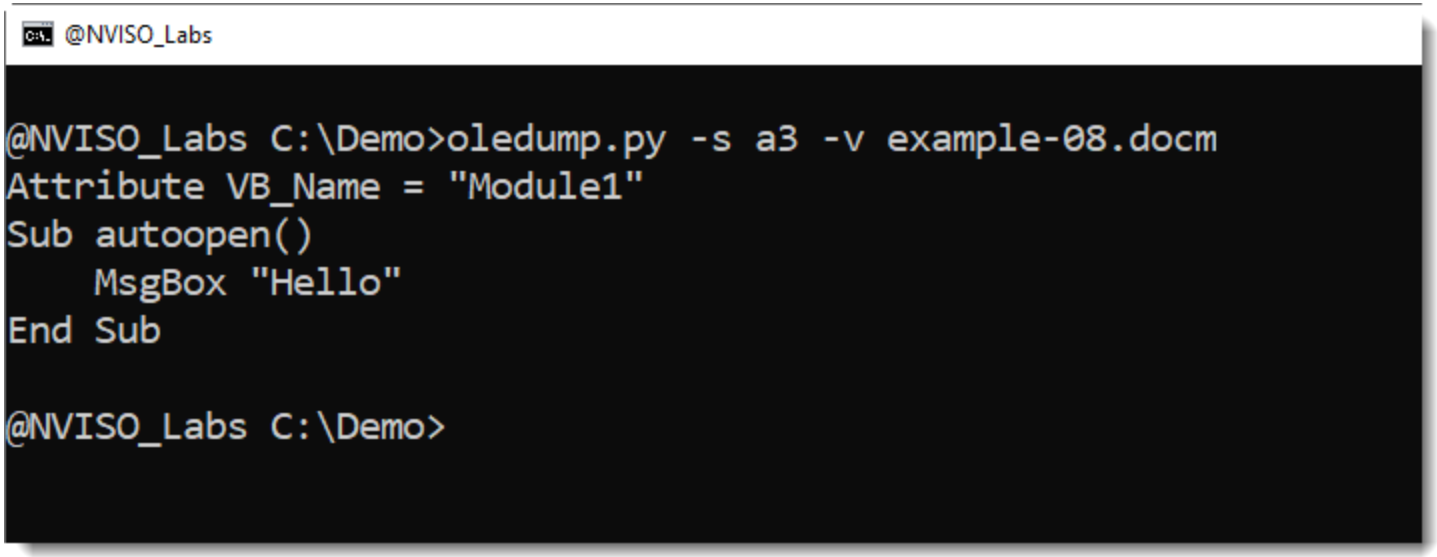
Example 5: Code signing tampering



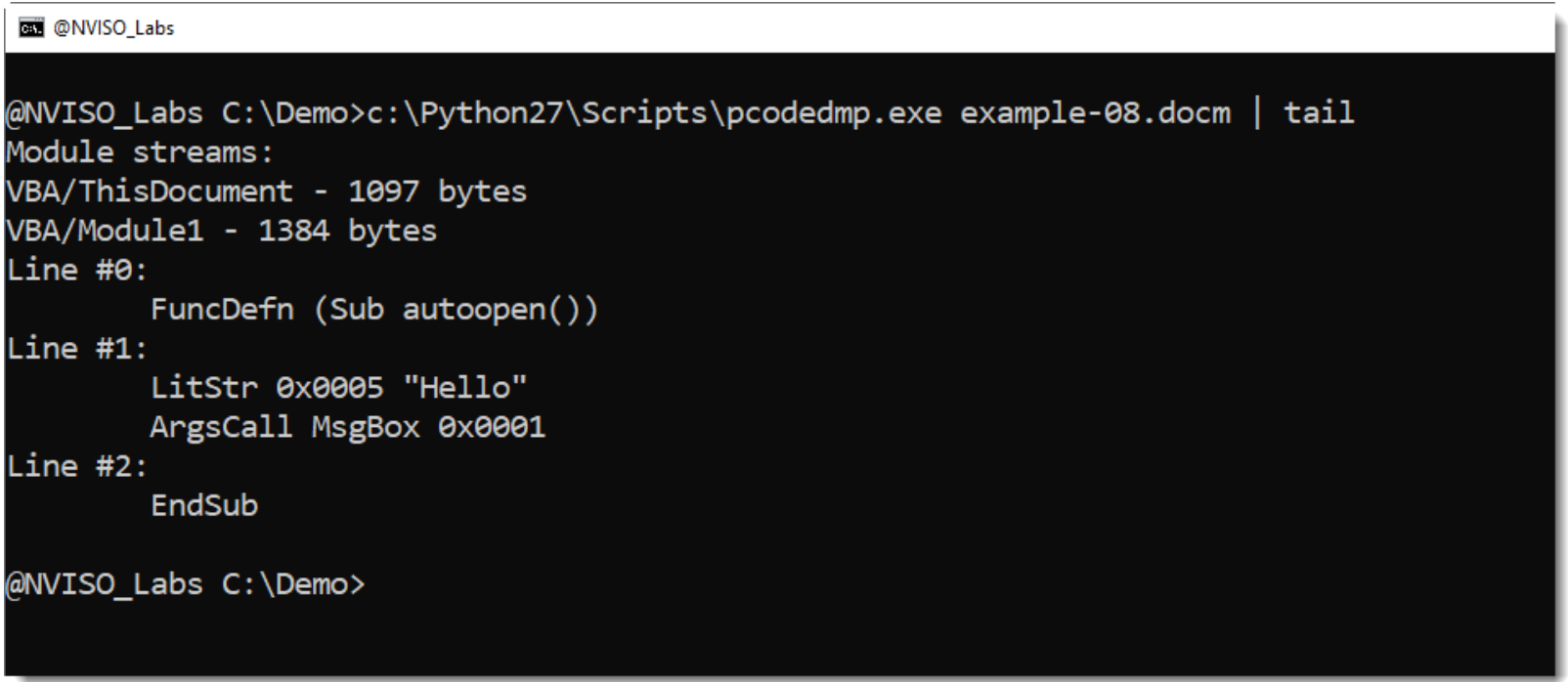
Example 5: Code signing tampering



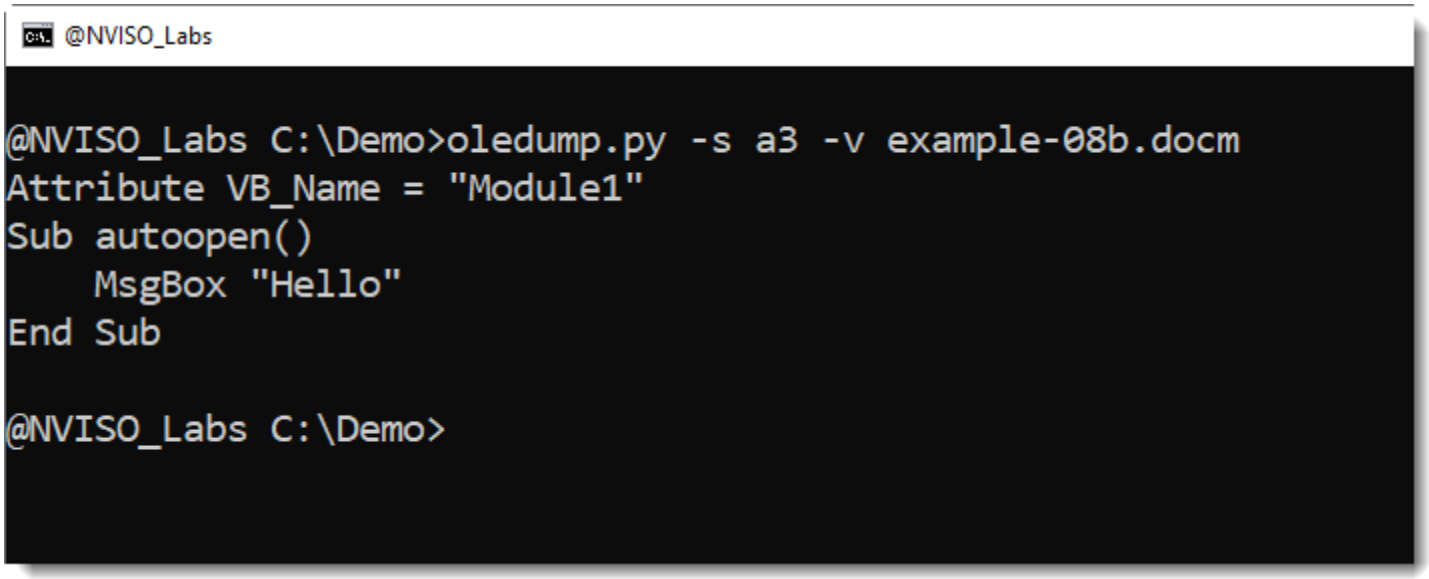
Example 5: Code signing tampering



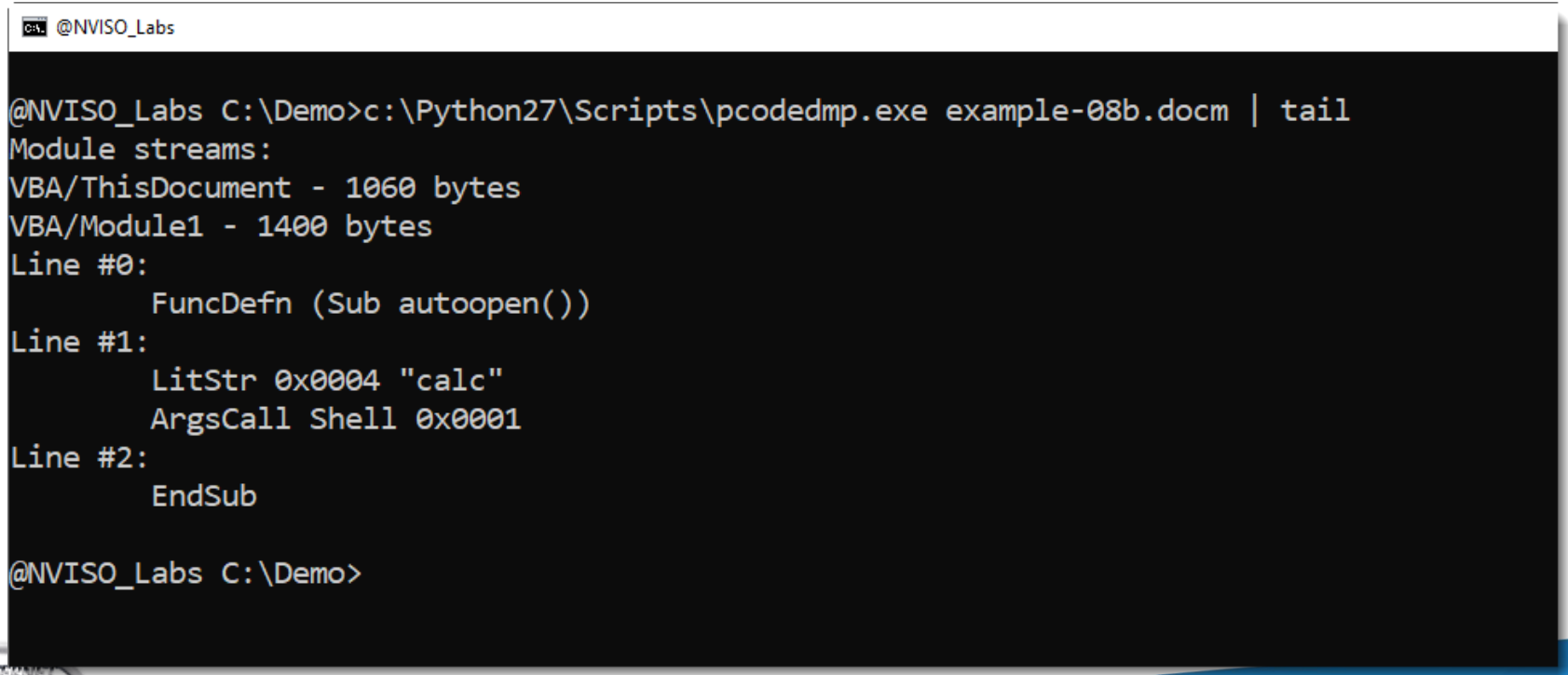
Example 5: Code signing tampering



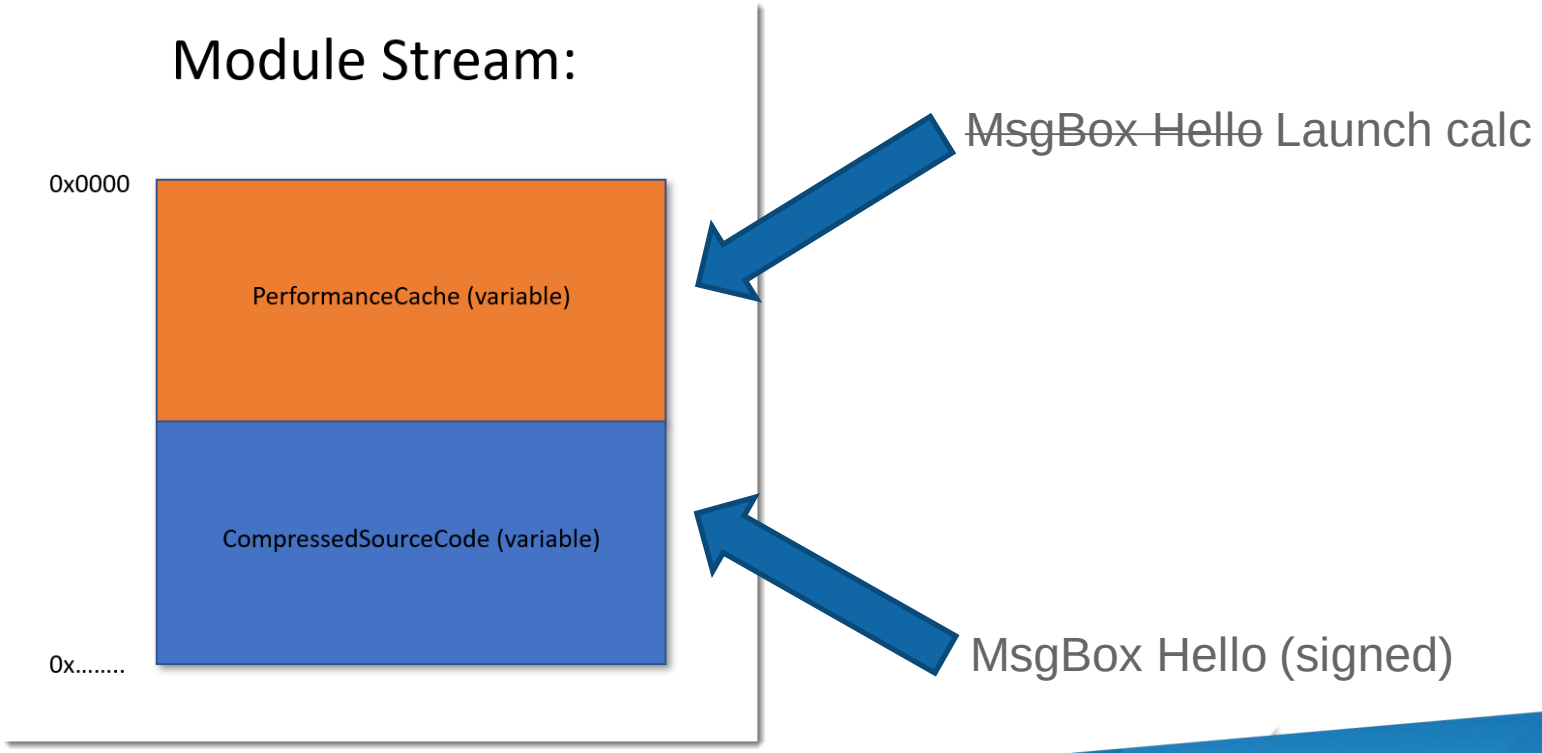
Example 5: Code signing tampering



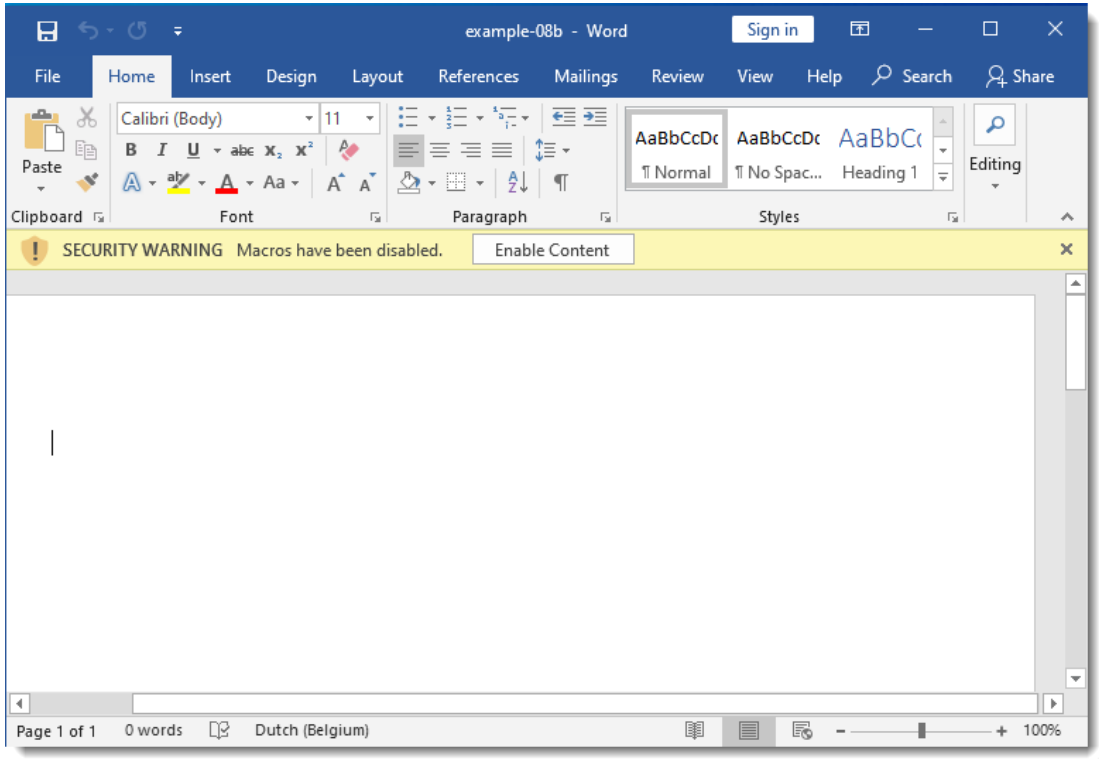
Example 5: Code signing tampering



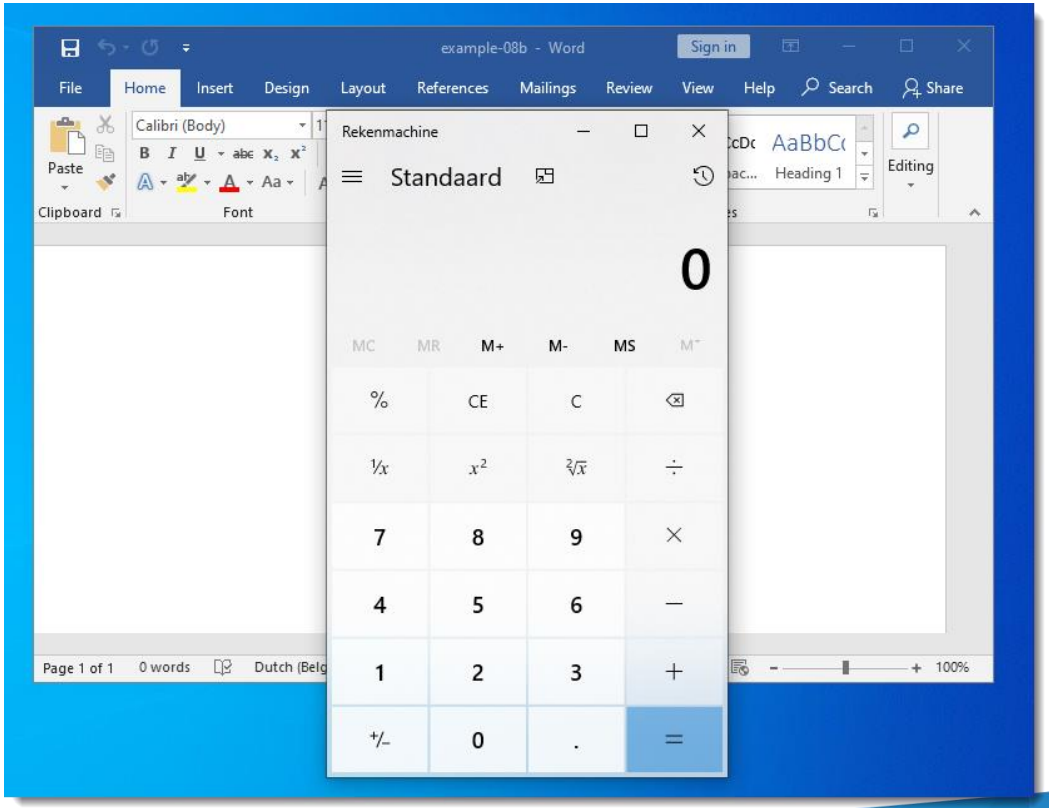
Example 5: Code signing tampering



Example 5: Code signing tampering



Example 5: Code signing tampering



Our Agenda

3 Other stuff …

Maldocs: a bit of blue, a bit of red

nviso

AutoCAD & VBA

Demo

https://isc.sans.edu/diary/Extracting+VBA+Macros+From+.DWG+Files/25634

Maldocs: a bit of blue, a bit of red

nviso

PDF & VBA (MS Office)

https://isc.sans.edu/forums/diary/PDF+maldoc1+maldoc2/20079/

PDF Encryption:

1) DRM

2) Confidentiality

Demo

https://isc.sans.edu/forums/diary/Encrypted+PDFs/23165/

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
```

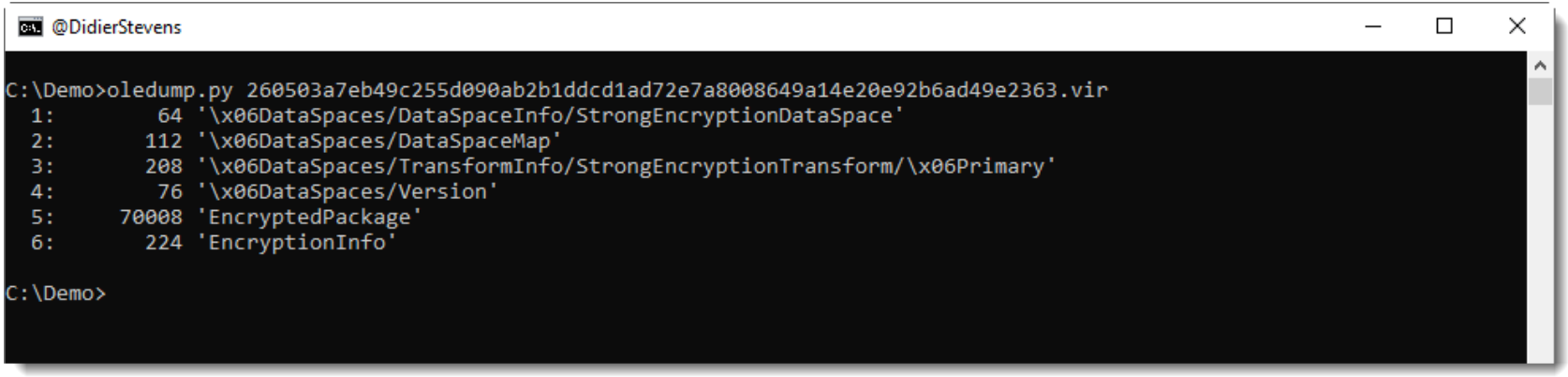
QPDF Confidentiality decryption:

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

MS Office Encryption
(VelvetSweatshop)

https://isc.sans.edu/forums/diary/VelvetSweatshop+Maldocs/24772/

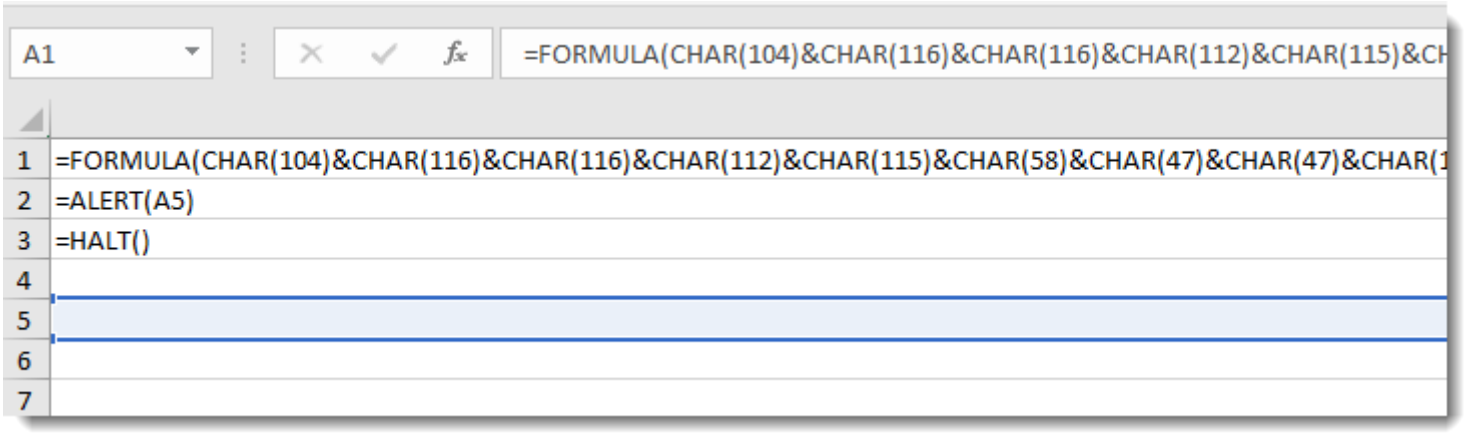
Maldocs: a bit of blue, a bit of red

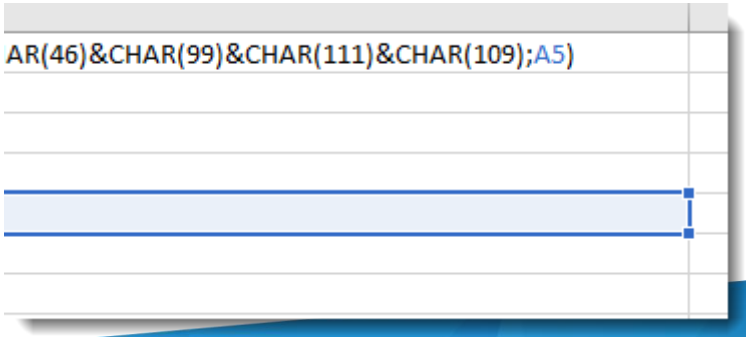


Maldocs: a bit of blue, a bit of red

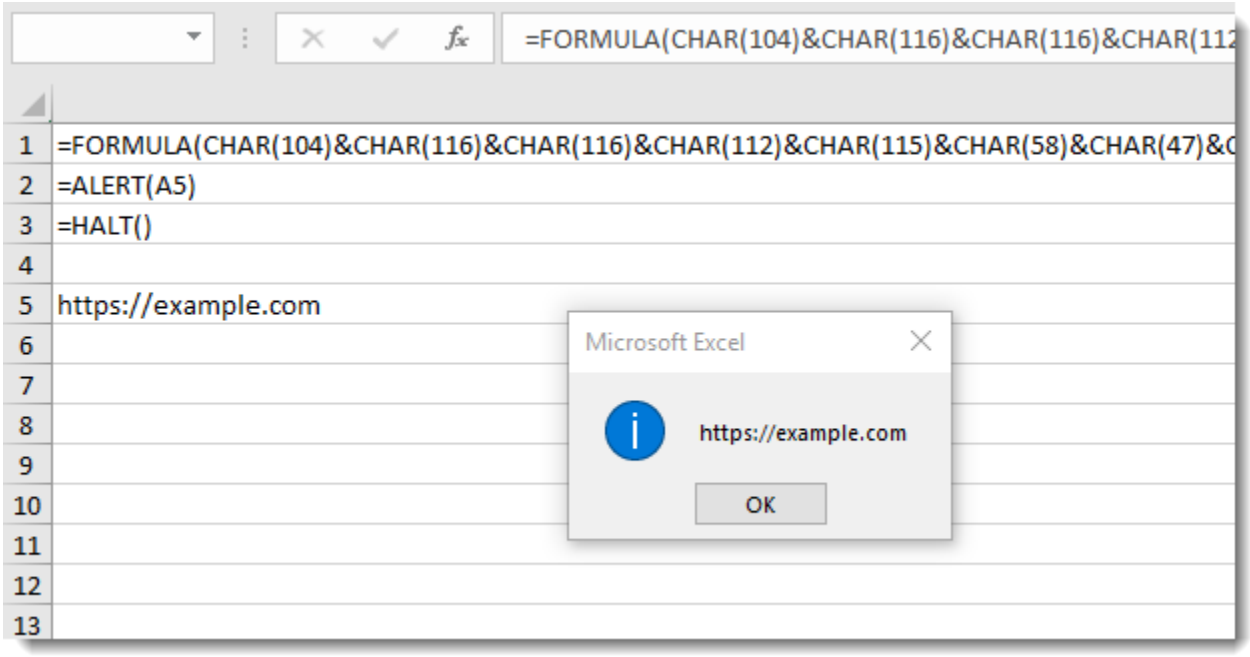
Excel 4 Macros:
Limiting the power of strings

Maldocs: a bit of blue, a bit of red

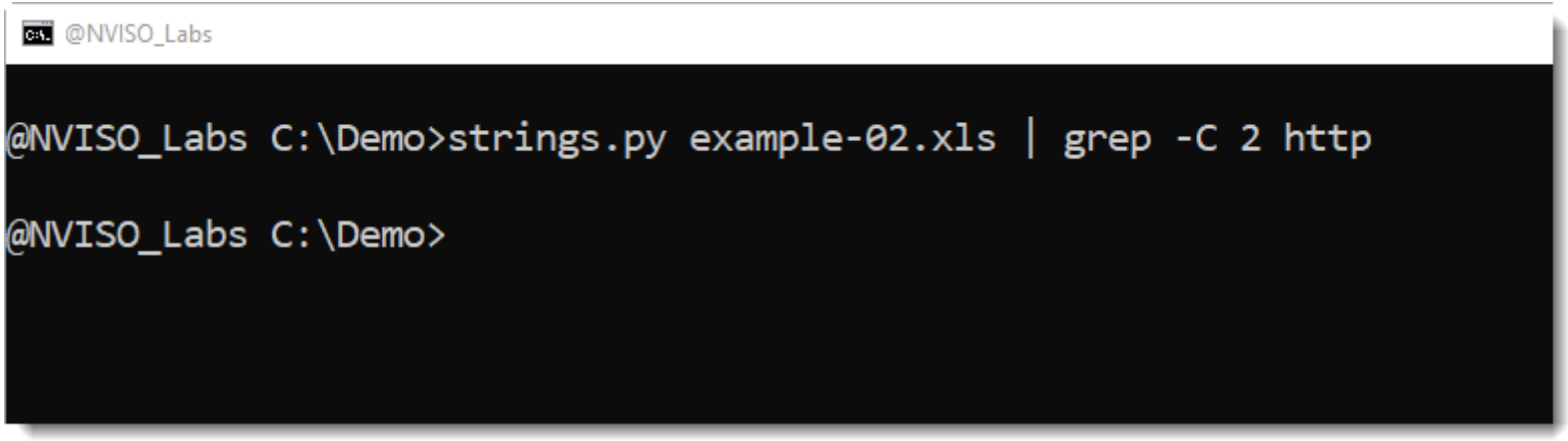




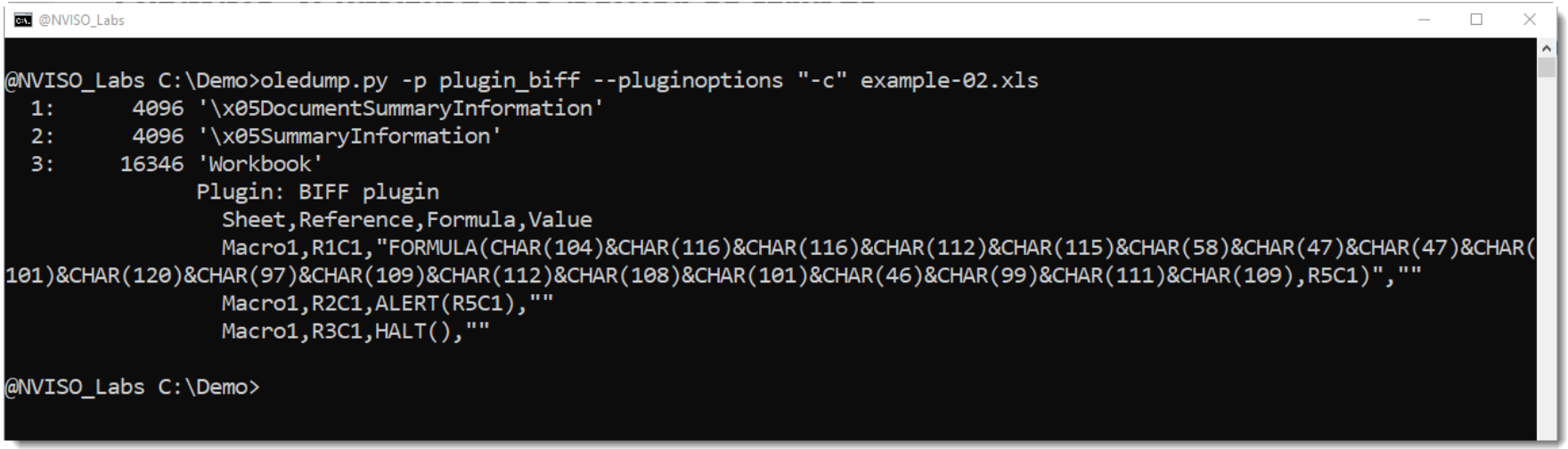
Maldocs: a bit of blue, a bit of red



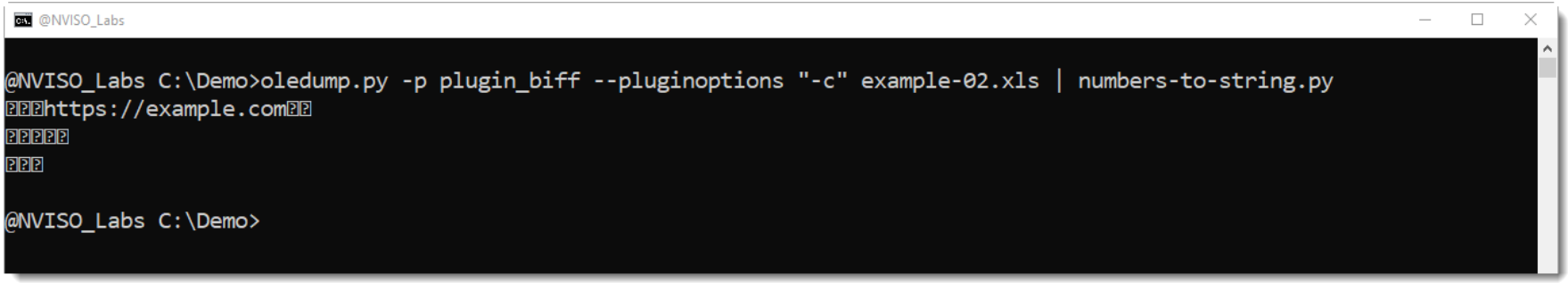
Maldocs: a bit of blue, a bit of red



Maldocs: a bit of blue, a bit of red



Maldocs: a bit of blue, a bit of red



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

www.nviso.eu

nviso