

Persisting with Microsoft Office: Abusing Extensibility Options

William Knowles

Labs

obligatory \$whoami



- William Knowles
- Security Consultant at MWR InfoSecurity
- @william_knows

Agenda

- DLL
- VBA
- COM
- VSTO
- Prevention and Detection

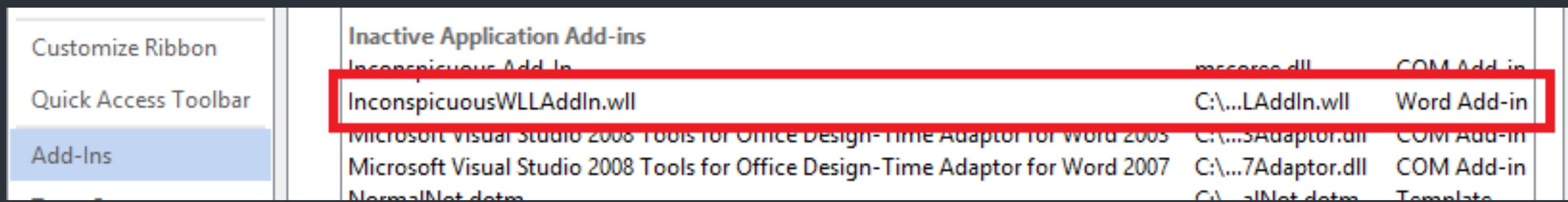
Motivations

- It's -everywhere- and it's got lots of use cases
- Office templates? What else?

Trusted Locations		
Warning: All these locations are treated as trusted sources for opening files. If you change or add a location, make sure that the new location is secure.		
Path	Description	Date Modified
User Locations		
C:\...\AppData\Roaming\Microsoft\Templates\	Word 2013 default location: User Templates	
C:\...\Files (x86)\Microsoft Office\Templates\	Word 2013 default location: Application Tem...	
C:\...\ata\Roaming\Microsoft\Word\Startup\	Word 2013 default location: StartUp	
Policy Locations		

Word ... Linked Libraries?

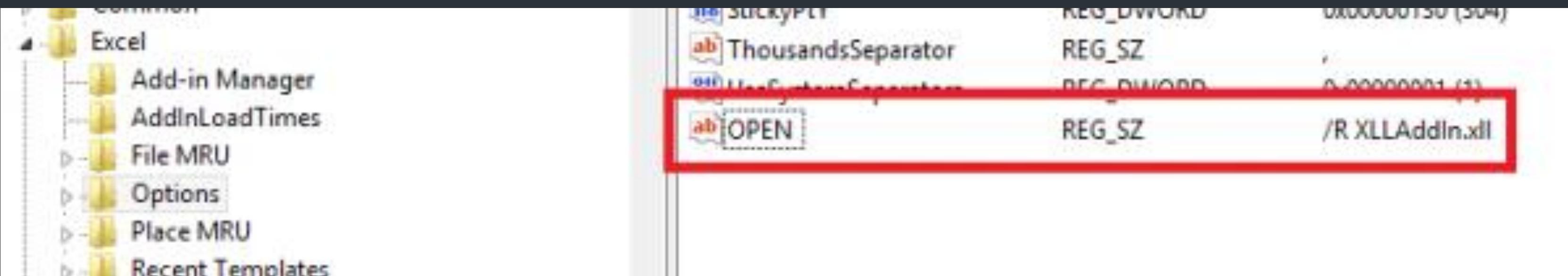
- It's just a DLL ...
- "... are standard Windows DLLs that implement and export specific methods to extend Word functionality"
- "... no enhancements and no documentation updates to Word WLLs since Microsoft Office 97"



Excel (XLL?) too ...

- Slightly more updated ... latest SDK from 2007.
- You need to export the right functions.
- Also slightly more configuration:

`HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Options`

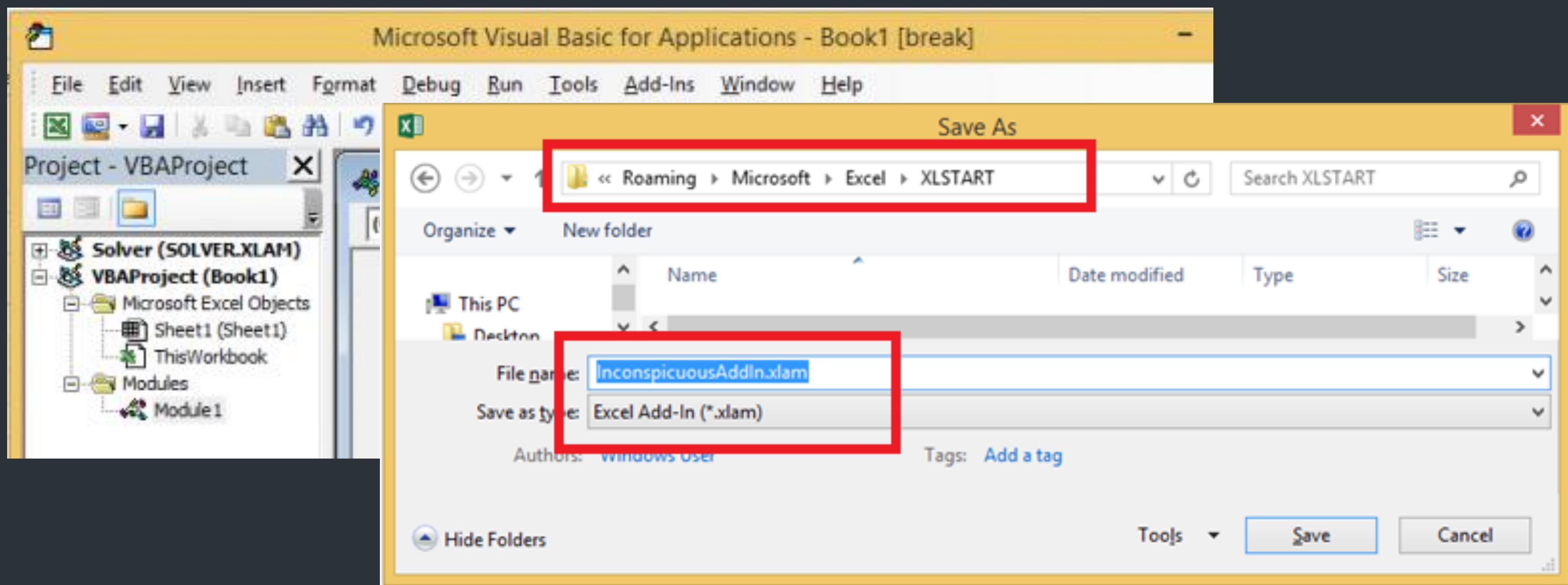


DLL Add-Ins
for Word and Excel

API3

Excel VBA Add-Ins

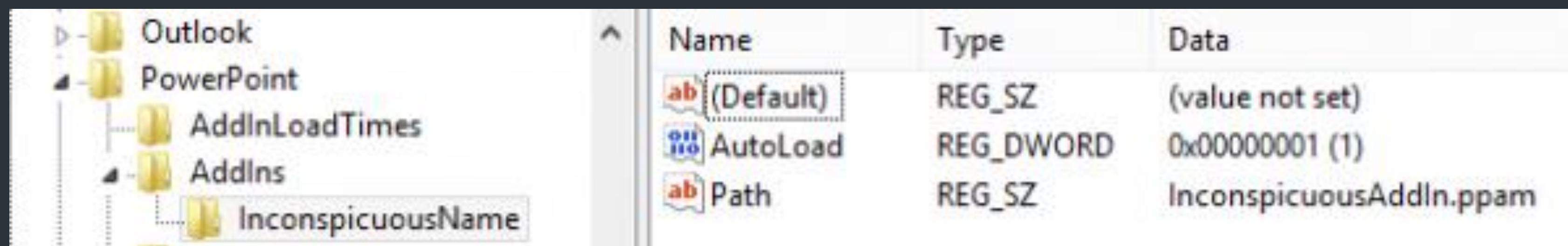
- It's all VBA, no spreadsheets.
- *.xla // *.xlam



PowerPoint VBA Add-Ins

- *.ppa // *.ppam
- Again, it's inconsistent, and needs manual configuration:

`HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\PowerPoint\AddIns\<AddInName>`



Name	Type	Data
(Default)	REG_SZ	(value not set)
AutoLoad	REG_DWORD	0x00000001 (1)
Path	REG_SZ	InconspicuousAddIn.pppam

VBA Add-Ins
for Excel and PowerPoint
... and others

API3

COM in Two Minutes

- Based on OLE and ActiveX – it's a standard to enable component interaction.
- COM objects, DLLs and .Net

COM Add-Ins for *

- COM – the legacy way is always a good way.
- The “**IDTExtensibility2**” interface.
- Registration can be problematic ...

`HKEY_CURRENT_USER\Software\Microsoft\Office\<Program>\Addins\<AddInName>`

- Register with “**regasm.exe /codebase InconspicuousAddIn.dll**”.

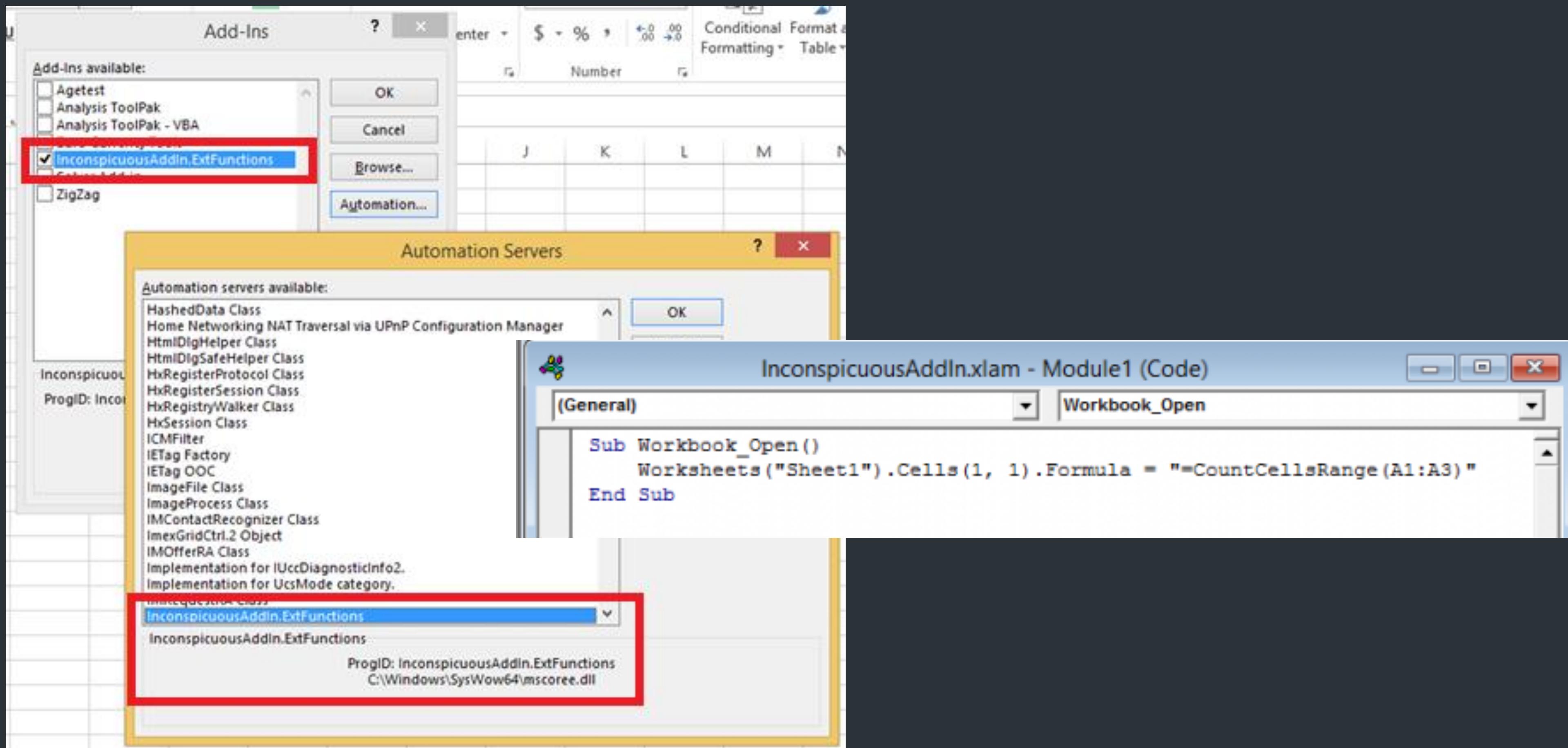
Name	Type	Data
ab(Default)	REG_SZ	(value not set)
abDescription	REG_SZ	Outlook Inconspicuous Addin
abFriendlyName	REG_SZ	Outlook Inconspicuous Addin
abLoadBehavior	REG_DWORD	0x00000003 (3)

- Specific COM use case - for user defined functions.

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Options

- Register again with “regasm.exe”.

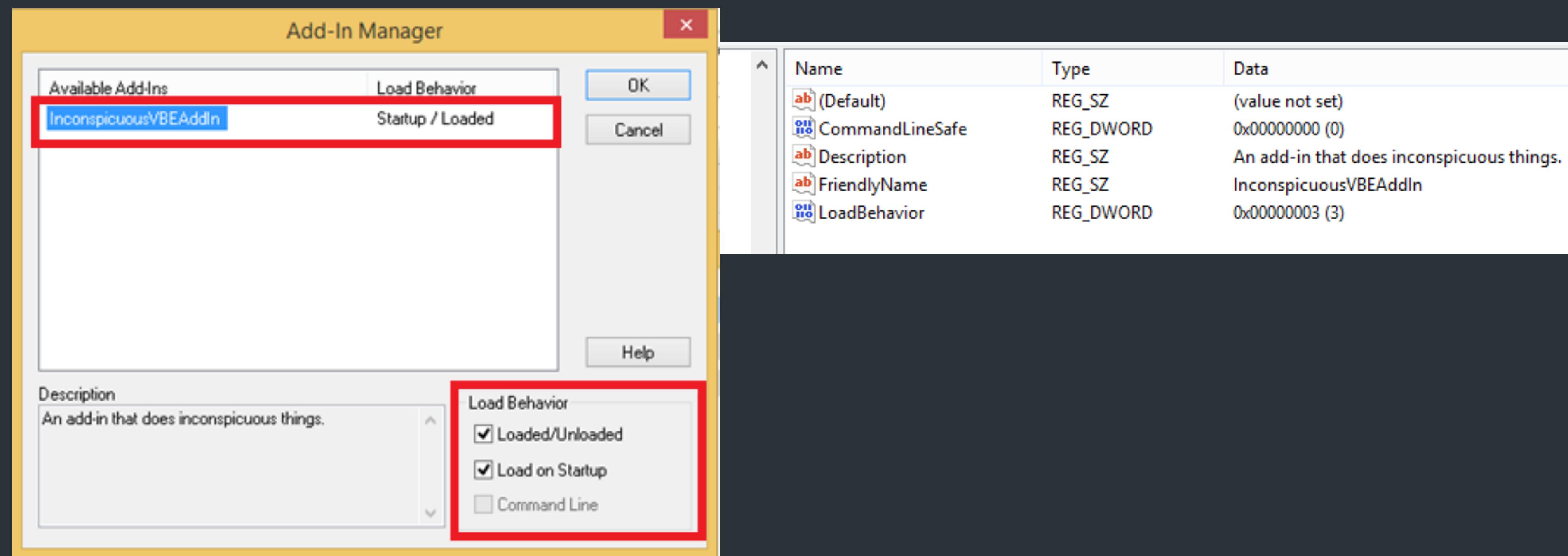
=sum(calc) with Excel Automation Add-Ins



Attacking VBA Snoopers with VBE Add-Ins

- Why? Why? Why?
- More registry edits, more “regasm.exe”

`HKEY_CURRENT_USER\Software\Microsoft\VBA\VBE\6.0\Addins\<VBEAddIn.Name>`



COM Add-Ins

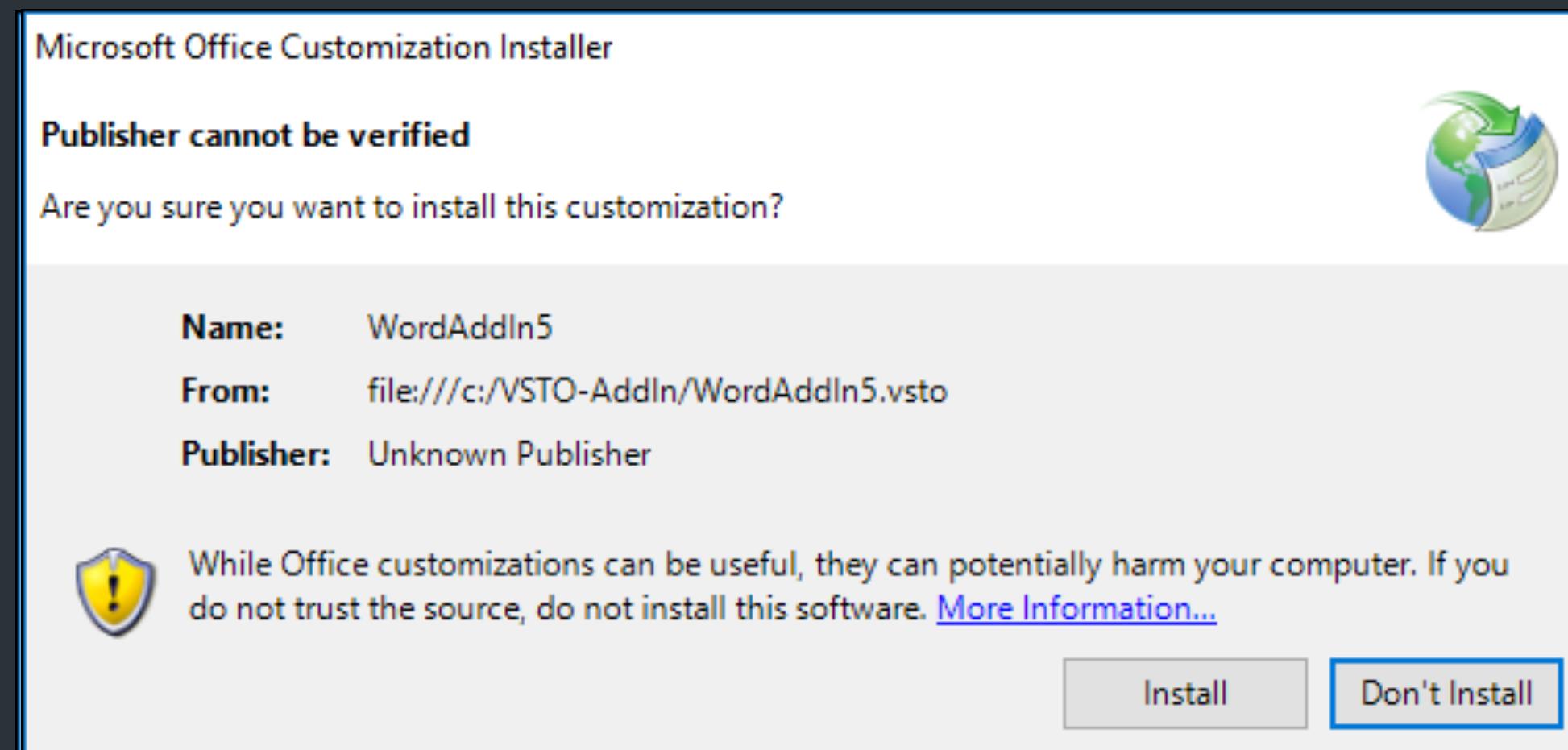
API3

* .VSTO

- Visual Studio Tools for Office – it's a COM replacement and requires a special runtime.

```
C:\>vstor_redist.exe /q /norestart
C:\>"C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\10.0\VSTOInstaller.exe" /i "c:\VSTO-AddIn\WordAddIn5.vsto"
```

- Build and install – very, very loudly.

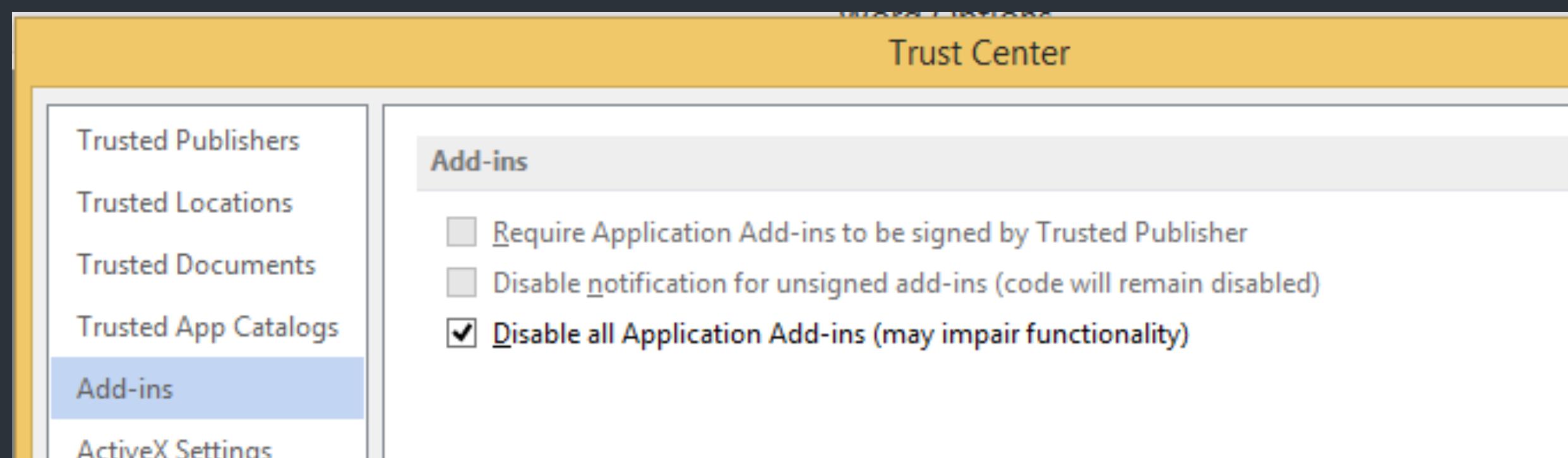


VSTO Add-Ins

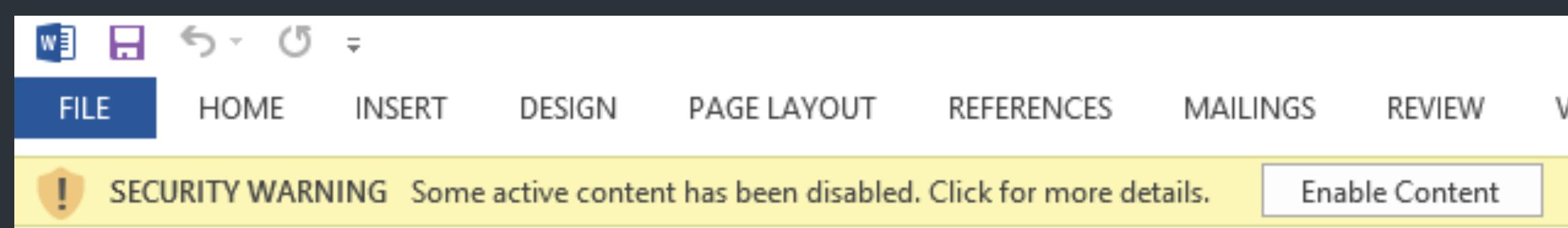
API3

Defending Against Malicious Add-Ins

- Easy for XLL, COM, Automation, and VSTO add-ins:



- If required – sign and disable notifications.



Defending Against Malicious Add-Ins



- For WLL and VBA add-ins ... not so much.
- (1) Remove or relocate trusted locations.
- (2) Detective capability:
 - Monitor trusted locations for changes
 - Monitor registry keys used to enable add-ins.
 - Process relationships.

Conclusion

@william_knows

API3