Persisting with Microsoft Office: Abusing Extensibility Options

William Knowles
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?
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
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>
VBA Add-Ins for Excel and PowerPoint ... and others
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”.

![Registry Keys and Values](image-url)
=sum(calc) with Excel Automation Add-Ins

- Specific COM use case – for user defined functions.

  HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Options

- Register again with “regasm.exe”.

![Register COM Components](image)
=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>
*.VSTO

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

```
C:\vstor_redist.exe /q /norestart
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

LABS
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