MWR Labs

One Template To Rule ‘Em All

Kostas Lintovois

28th October 2016

#t2’16.infosec

MWR LABS

++

Outline

- Quick Macros and Office GPOs recap
- Office Trusts and Templates
- VDIs and covert persistence with Templates
- Raising the bar – Application Control & EMET
- EMET Configuration Abuse
- WePWNise demo
- Conclusions & Questions

++

Visual Basic for Applications (VBA)

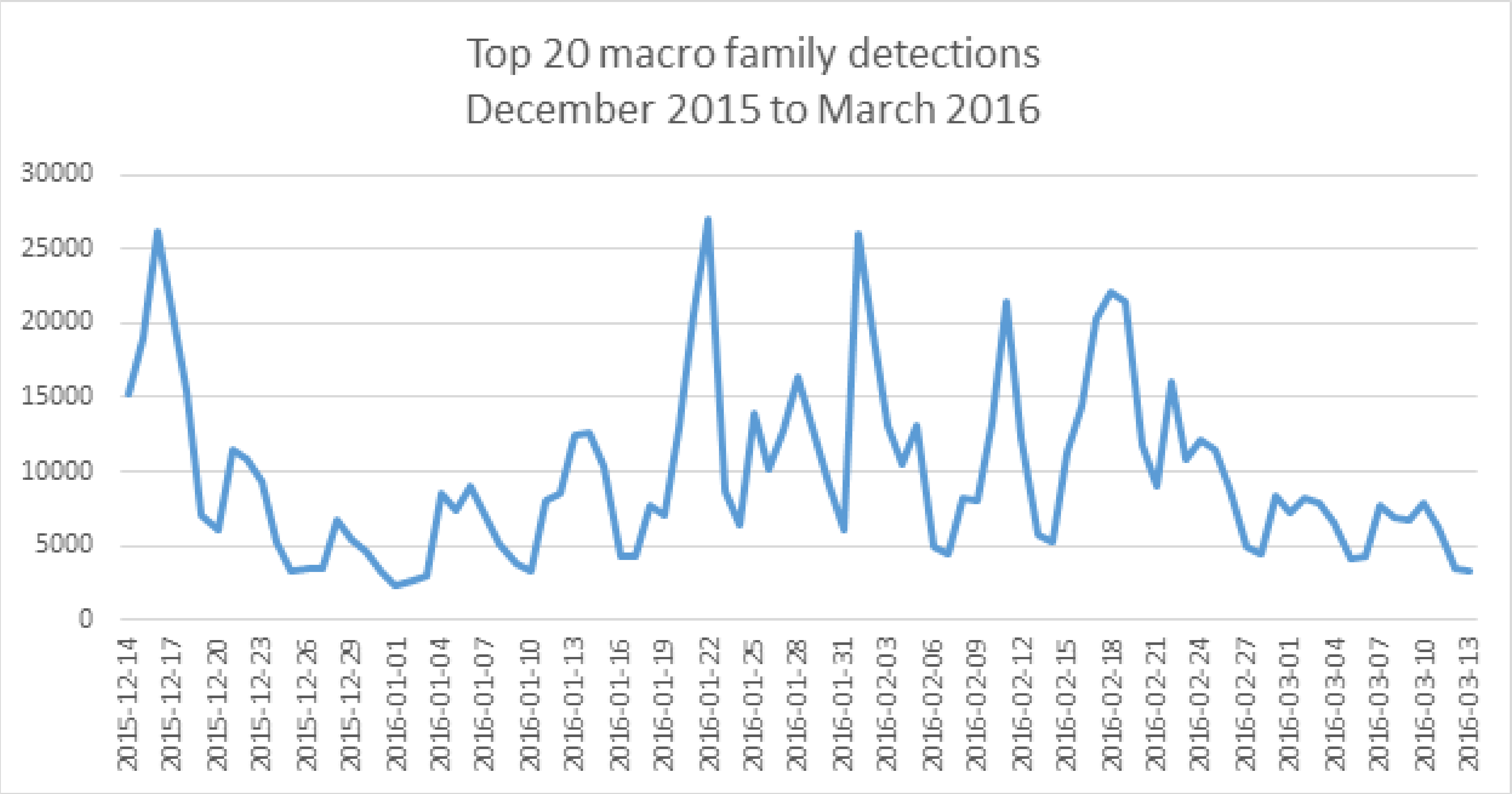
- The VBA component is installed by default as part of Office’s installation
- VBA enables the use of multiple technologies
- Office settings can be controlled locally or via GPO

Macros recap

++

Visual Basic for Applications (VBA)

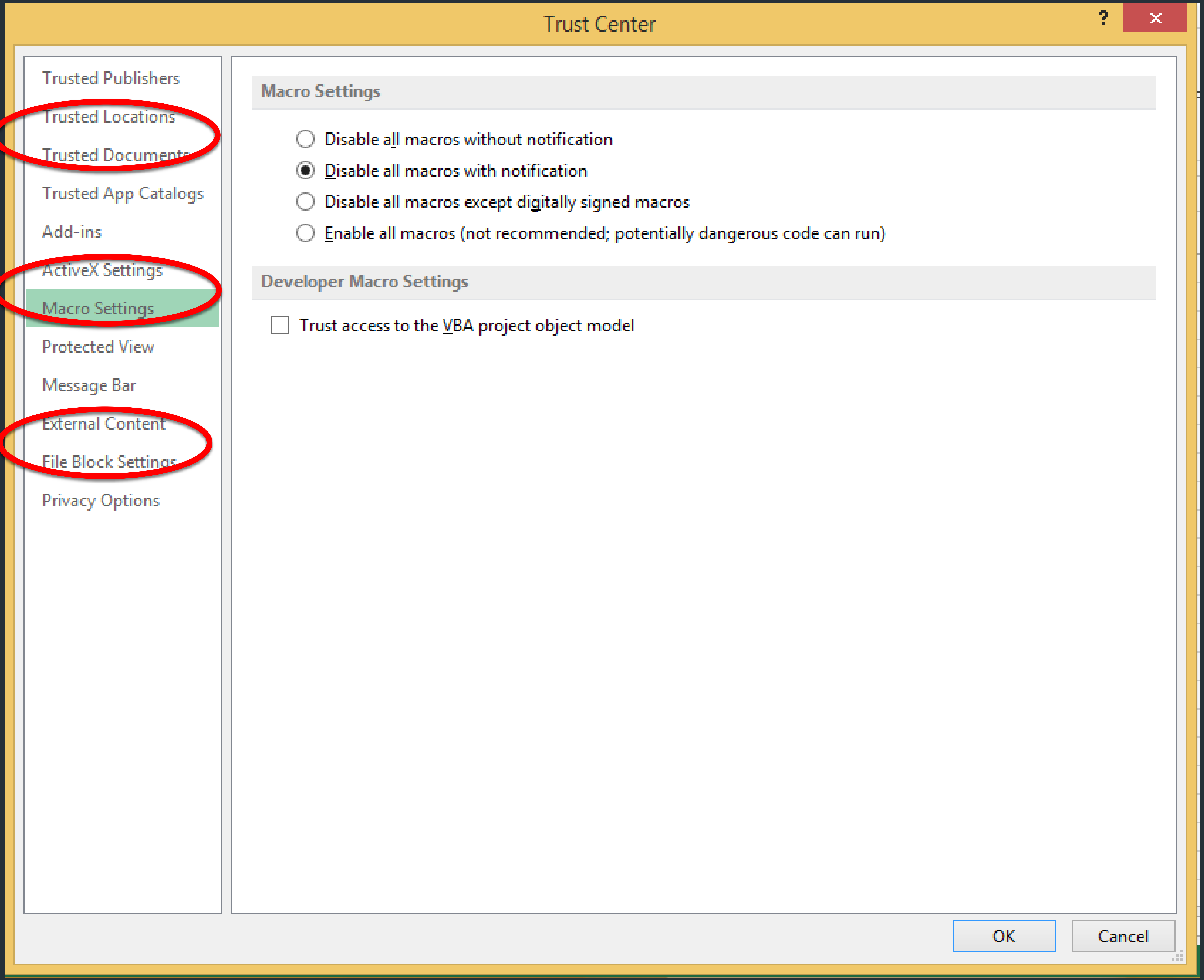
+ Macro-based malware infections are still increasing



Macros recap

++

Macros security settings



Macro Settings

○ Disable all macros without notification

● Disable all macros with notification

○ Disable all macros except digitally signed macros

○ Enable all macros (not recommended; potentially dangerous code can run)

Developer Macro Settings

□ Trust access to the VBA project object model

++

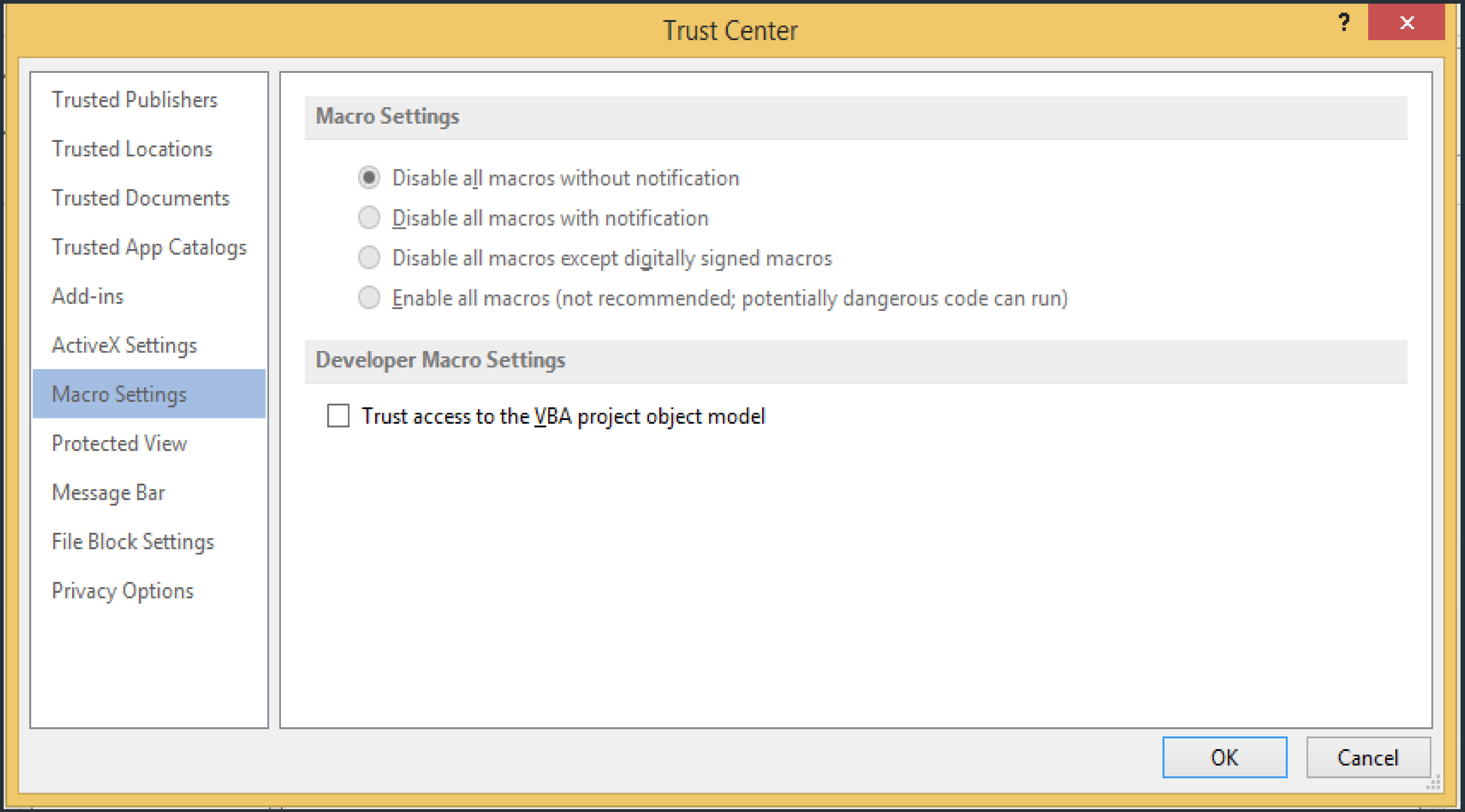
Office settings via GPO

- Every Office version ships with its own GPO Templates (ADMX/ADML)
- Multiple settings within the GPO
  - Machine > Administrative Templates > Microsoft Office {version}
  - User > Administrative Templates > Microsoft Office {version} > Security Settings
  - User > Administrative Templates > AppName {version} > AppName Options > Security > Trust Center

Macros recap

++

Office settings via GPO



Macro Settings

● Disable all macros without notification

○ Disable all macros with notification

○ Disable all macros except digitally signed macros

○ Enable all macros (not recommended; potentially dangerous code can run)

Developer Macro Settings

□ Trust access to the VBA project object model

++

Too many trusts

- Trusted Locations
- Trusted Documents
- Trusted Publishers
- Trusted App Catalogs

Office Trusts and Templates

Trusted Locations

- Trusted locations are paths where security policies do not apply
- Each Office application comes with its own predefined set of trusted locations, including user writable paths ...
  - {User Home}\AppData\Roaming\Microsoft\Templates
  - {User Home}\AppData\Roaming\Microsoft\Word\Startup
  - {User Home}\AppData\Roaming\Microsoft\Excel\XLSTART

++

Trusted Locations GPOs

+ Trusted locations can be controlled via GPO

+ Settings are defined within the user’s GPO branch

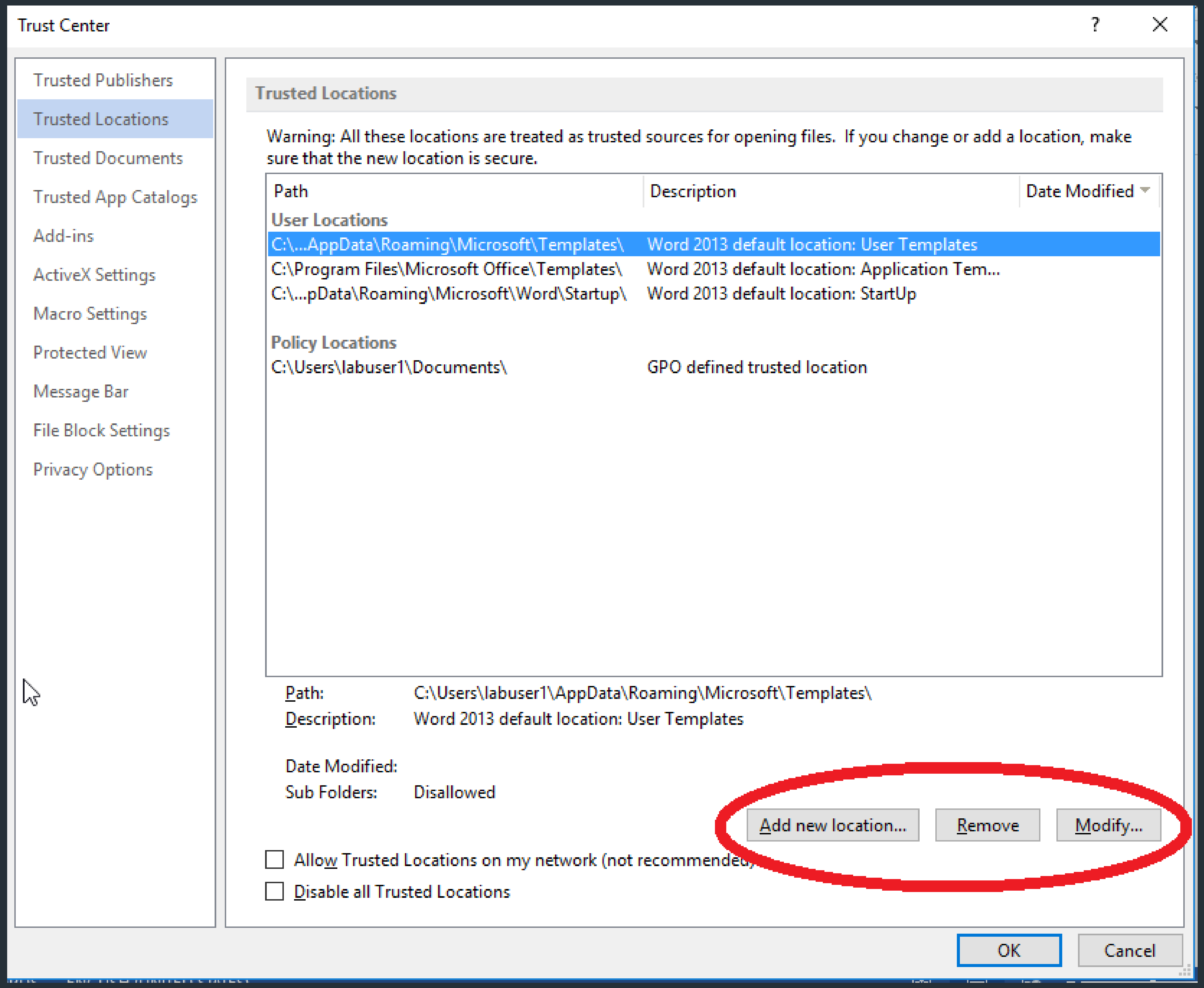
  + User > Administrative Templates > AppName {version} > AppName Options > Security Settings > Trust Center > Trusted Locations

  + User > Administrative Templates > Office {version} > Security Settings > Trust Center

Office Trusts and Templates

++

Trusted Locations GPOs



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.

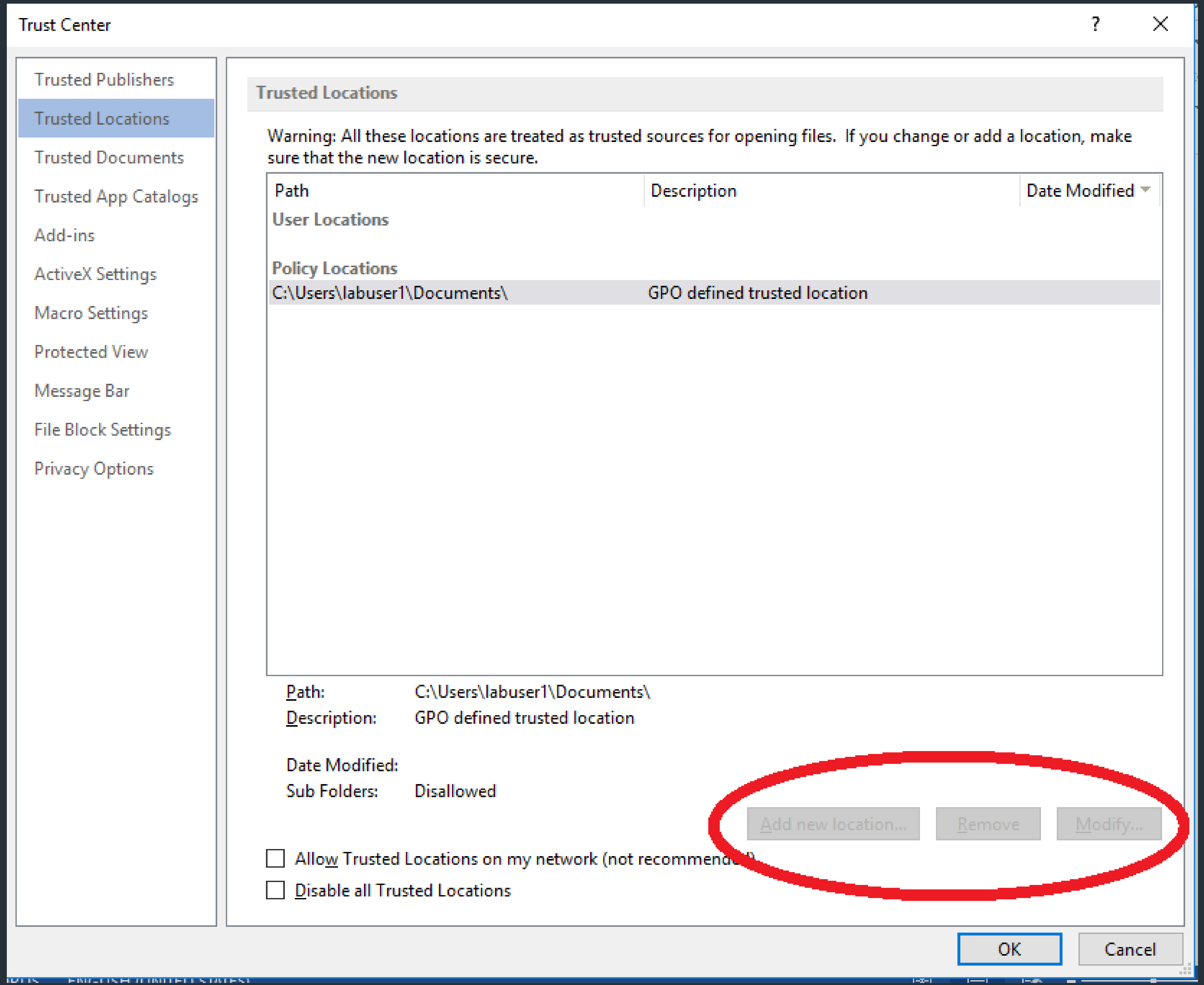
Path	Description	Date Modified
User Locations		
C:\...AppData\Roaming\Microsoft\Templates\	Word 2013 default location: User Templates	
C:\Program Files\Microsoft Office\Templates\	Word 2013 default location: Application Tem...	
C:\...pData\Roaming\Microsoft\Word\Startup\	Word 2013 default location: StartUp	
Policy Locations		
C:\Users\labuser1\Documents\	GPO defined trusted location	

Path: C:\Users\labuser1\AppData\Roaming\Microsoft\Templates\
Description: Word 2013 default location: User Templates

Date Modified:
Sub Folders: Disallowed

☐ Allow Trusted Locations on my network (not recommended)
☐ Disable all Trusted Locations

VS



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		
Policy Locations		
C:\Users\labuser1\Documents\	GPO defined trusted location	

Path: C:\Users\labuser1\Documents\
Description: GPO defined trusted location

Date Modified:
Sub Folders: Disallowed

☐ Allow Trusted Locations on my network (not recommended)
☐ Disable all Trusted Locations

++

Trusted Documents and more

+ Trusted Documents are files containing active content that has been enabled by the user

+ Trusted Publishers are entities provided with digital certificates that can be used to sign code

+ Trusted Add-ins enable the extension of functionality of Office applications using web technologies

++

Templates

- Templates are special Office files that formalise presentation and extend document actions
- All Office applications have their own template types (dot, xlt, dotm, xltm, oft)
- All Template locations include user writable trusted locations
  - {User Home}\AppData\Roaming\Microsoft\Templates
  - {User Home}\AppData\Roaming\Microsoft\Word\Startup
  - {User Home}\AppData\Roaming\Microsoft\Excel\XSLSTART
- Templates use is a common practice in enterprise environments
- All Office applications have a number of predefined handler functions that are triggered upon certain actions (Document_New, Workbook_Open, Application_Startup, NewMailEx etc)

VDIs and persistence

++

Virtual Desktop Infrastructure (VDI)

- Centralised IT desktop management
- Reduced cost and hardware
- Increased mobility and remote access

CITRIX® XenDesktop

vmware® Horizon View

++

VDI persistence challenges

- Registry/File system do not persist across reboots
- Services/Scheduled tasks are not maintained either
- Only a subset of the user’s profile is remapped across sessions. This typically includes trusted locations ;)

++

Template Persistence

- By design provides an asynchronous invocation mechanism
- VBA functionality hooks on a number of events (Open,Close,New etc)
- Trusted locations are not typically evaluated as start-up items
- Macro enabled templates are not deemed as executable types
- Templates can be password protected to defend against automated analysis
- If a writable Template location is shared ==

++

Raising the bar – Application Control

+ Prevents unauthorised software from running
+ Doesn't affect macros as Office binaries have to be whitelisted
+ It can be effective in restricting other MS binaries (e.g. powershell.exe, rundll32.exe, regsvr32.exe, installutil.exe, regasm.exe ...)

++

Raising the bar – EMET

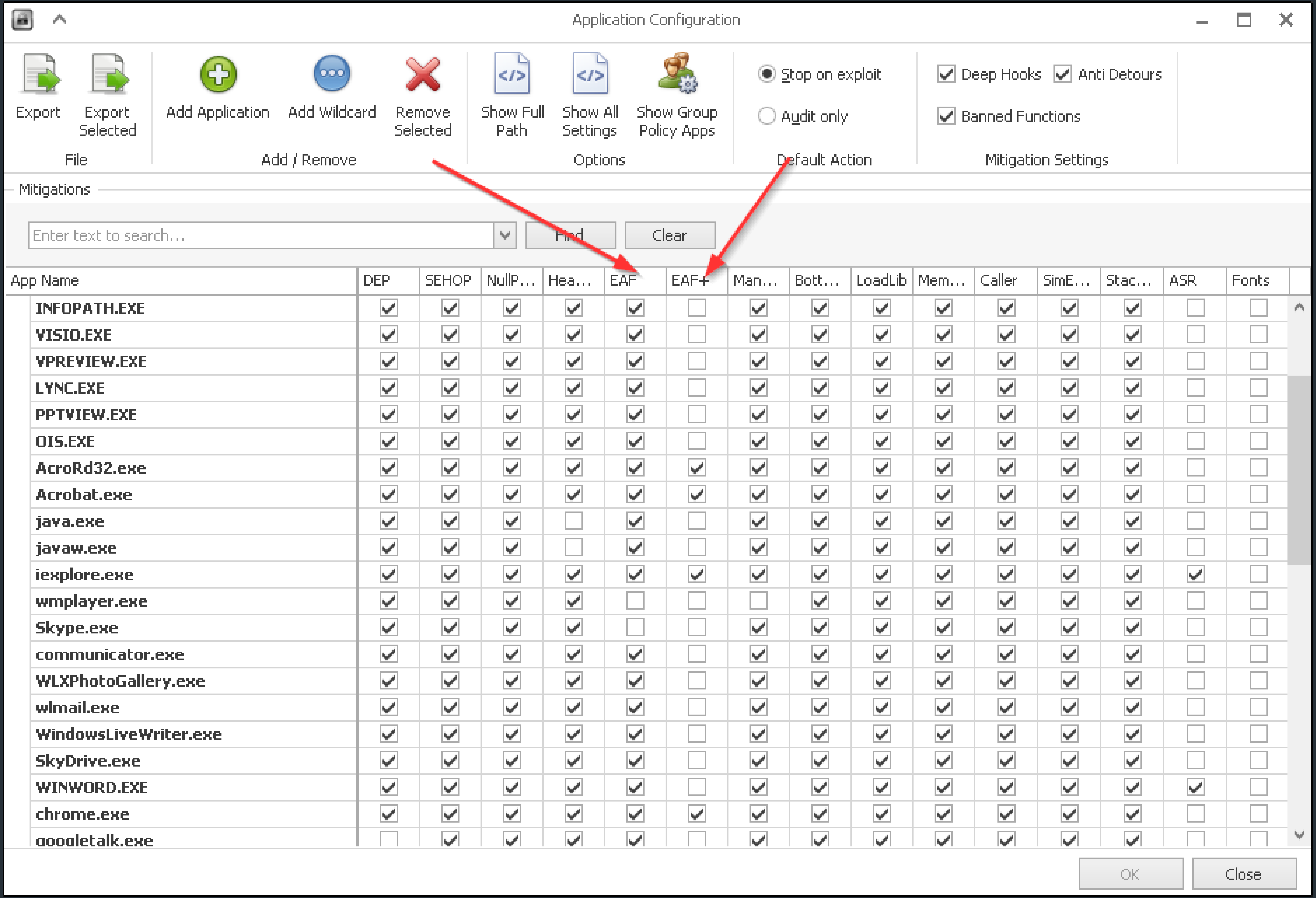
- Enhanced Mitigation Experience Toolkit
- Makes memory corruption exploitation harder
- Export Address Table Filtering (EAF)
- Not designed to prevent VBA Code execution

What is EMET?

MWR LABS

++

Raising the bar – EMET



● Stop on exploit
○ Audit only

Default Action

☑ Deep Hooks ☑ Anti Detours
☑ Banned Functions

Mitigation Settings

Mitigations

Enter text to search...

App Name	DEP	SEHOP	NullP...	Hea...	EAF	EAF+	Man...	Bott...	LoadLib	Mem...	Caller	SimE...	Stac...	ASR	Fonts
INFOPATH.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□	□
VISIO.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□	□
VPREVIEW.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□	□
LYNC.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□	□
PPTVIEW.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□	□
OIS.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□	□
AcroRd32.exe	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□	□
Acrobat.exe	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□	□
java.exe	☑	☑	☑	□	☑	□	☑	☑	☑	☑	☑	☑	☑	□	□
javaw.exe	☑	☑	☑	□	☑	□	☑	☑	☑	☑	☑	☑	☑	□	□
iexplore.exe	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□
wmplayer.exe	☑	☑	☑	☑	□	□	□	☑	☑	☑	☑	☑	☑	□	□
Skype.exe	☑	☑	☑	☑	□	□	☑	☑	☑	☑	☑	☑	☑	□	□
communicator.exe	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□	□
WLXPhotoGallery.exe	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□	□
wlmail.exe	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□	□
WindowsLiveWriter.exe	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□	□
SkyDrive.exe	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□	□
WINWORD.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	☑	□
chrome.exe	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□	□
googletalk.exe	□	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□	□

++

Current Macro Payloads (Metasploit)

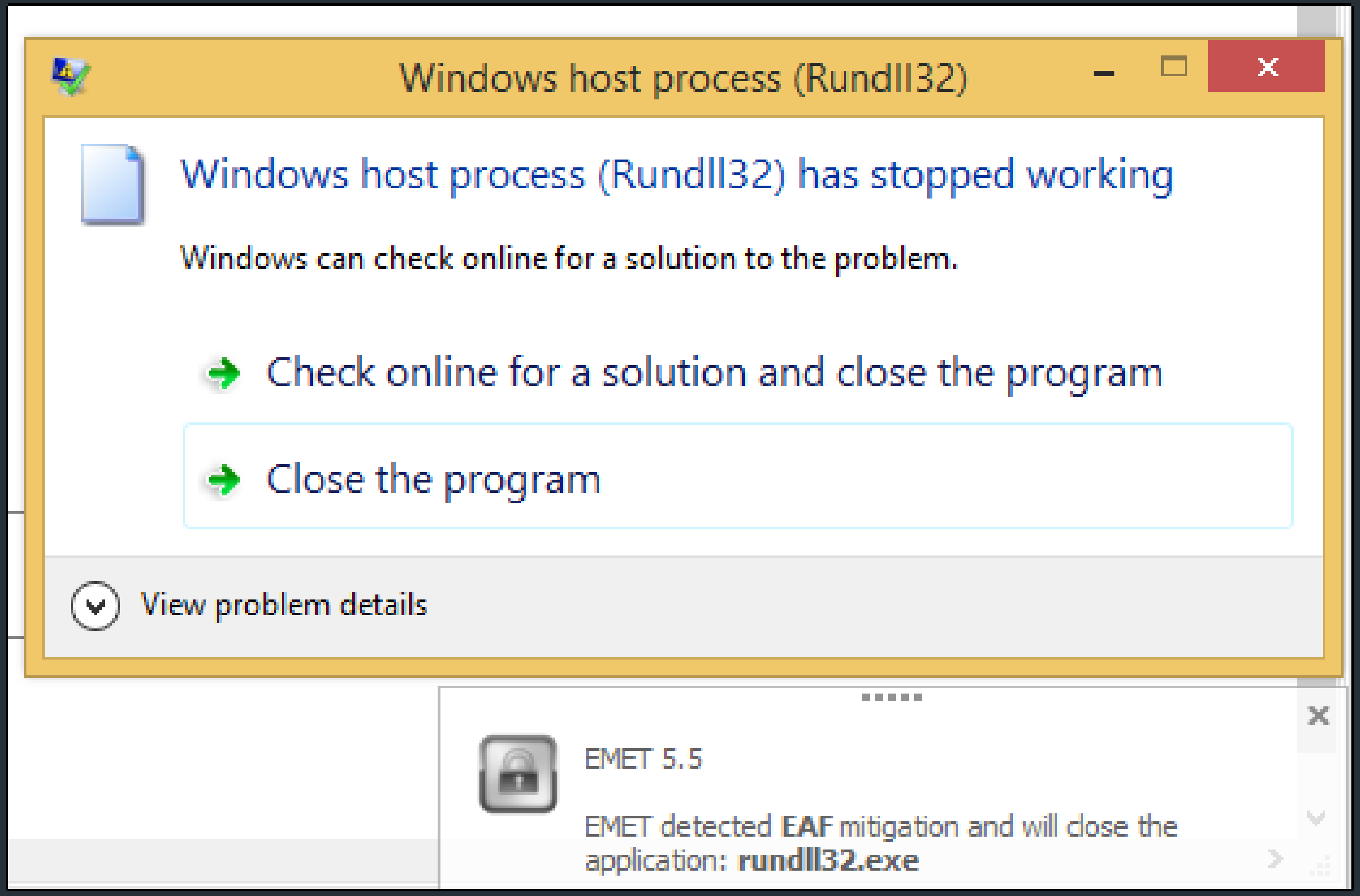
- VBA-PSH: Spawns PowerShell and injects shellcode
- VBA-EXE: Drops executable & runs it
- VBA: Injects shellcode into WINWORD.exe

Existing Implants

MWR LABS

++ Current Macro Payloads (Cobalt Strike / Empire)

- CS: Injects into Rundll32.exe
- Empire: Wraps around powershell.exe



Windows host process (Rundll32)

Windows host process (Rundll32) has stopped working

Windows can check online for a solution to the problem.

EMET 5.5

EMET detected **EAF** mitigation and will close the application: **rundll32.exe**

++

Introducing WePWNise

- + VBA code generation
- + Configuration enumeration
- + Weakness identification
- + Dynamic payload injection
- + Integration

++

Configuration Weakness Exploitation

- Enumerates Registry settings
- Bypasses SRPs & EMET protected paths
- Injection via WINAPI calls in VBA

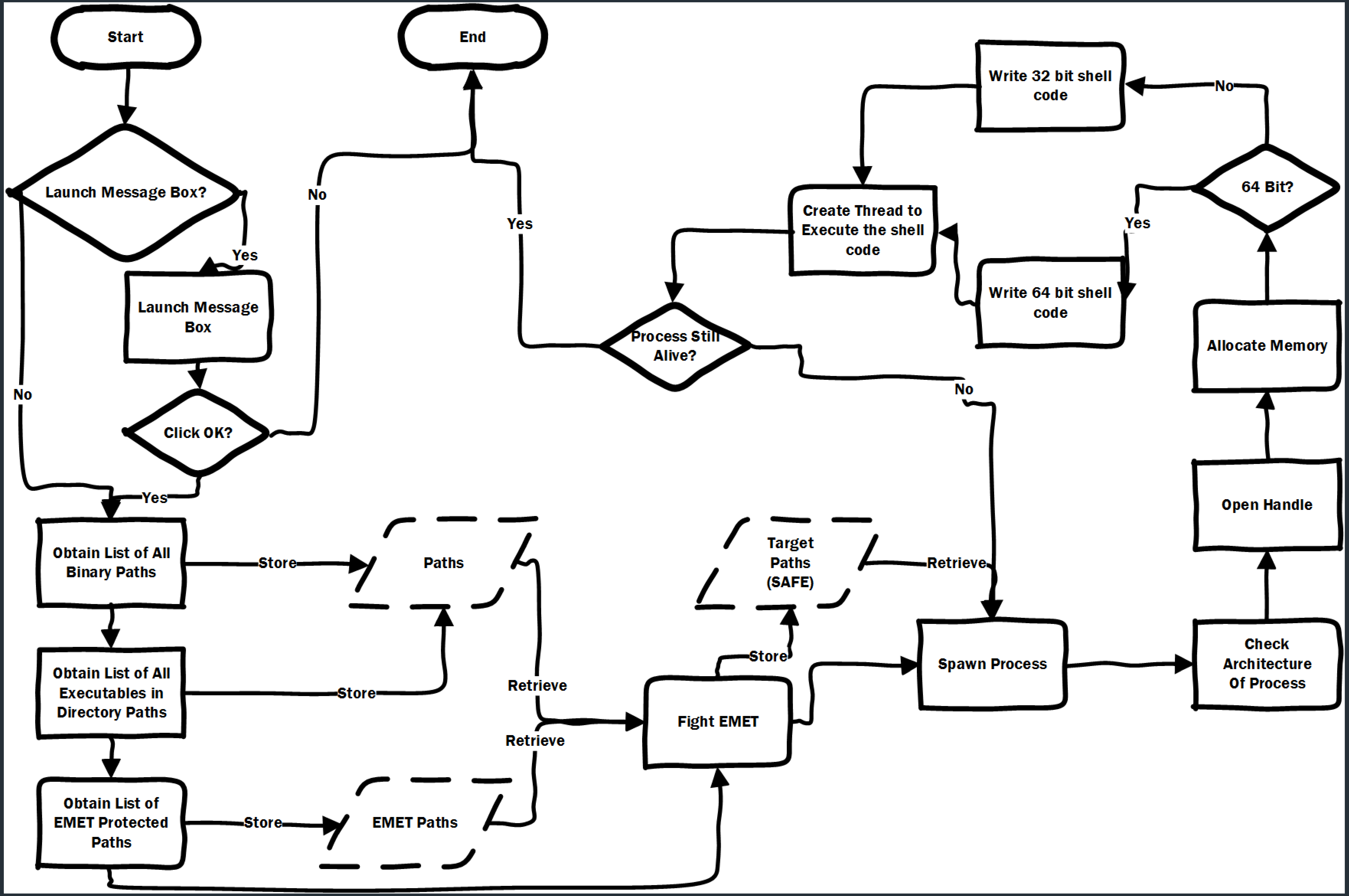
++

How does WePWNise inject?

- Native VBA code
- CreateProcessA
- VirtualAllocEx
- WriteProcessMemory
- CreateRemoteThread

++

WePWNise Map



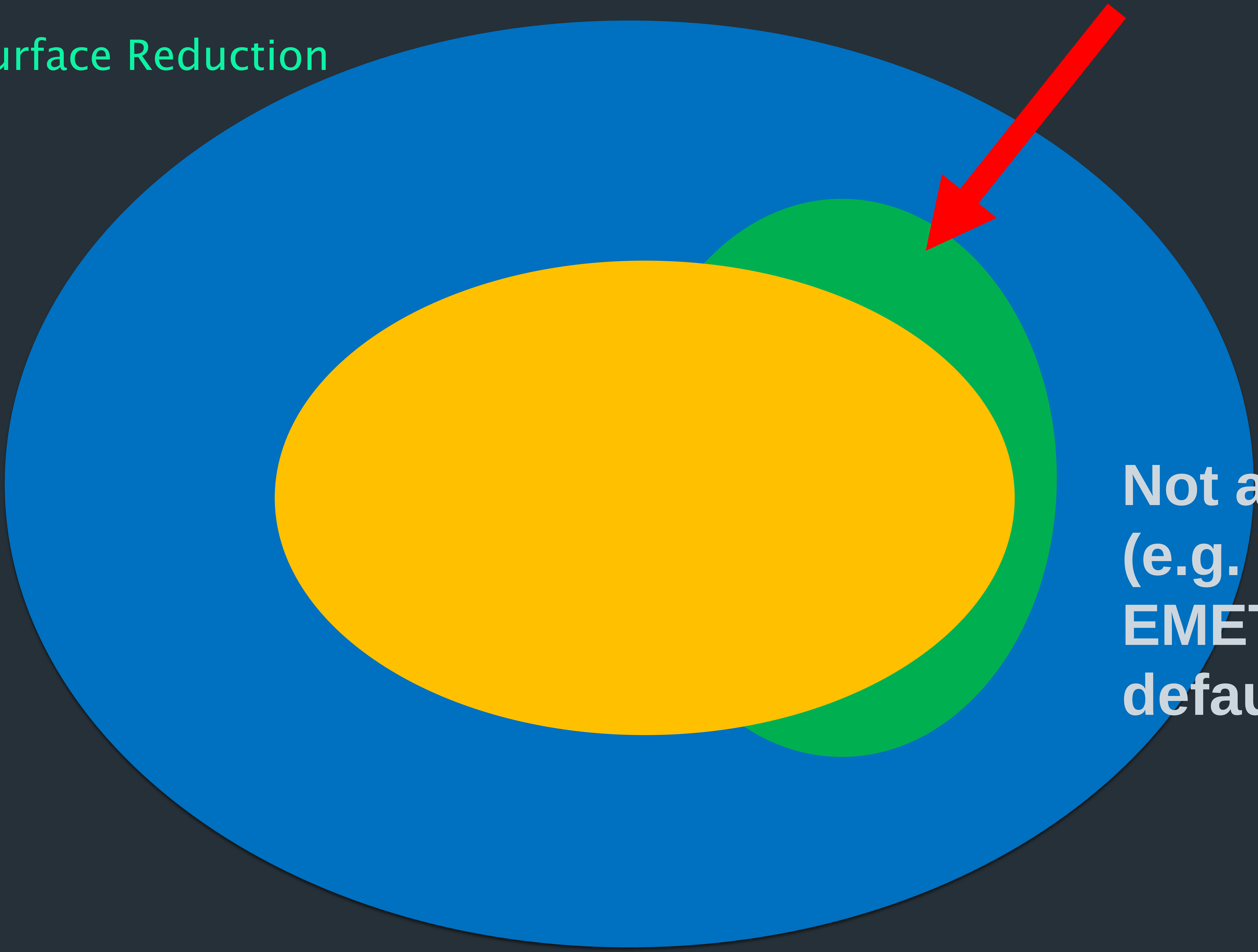
++

Enumeration

+ Native Registry Calls (Wscript.Shell)
+ HKLM\SOFTWARE\Microsoft\EMET\AppSettings
+ HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer
+ Metasploit:

```
> post/windows/gather/enum_emet
> post/windows/gather/enum_trusted_locations
```

++ Attack Surface Reduction



Not all binaries can be protected (e.g. VPN agents, Skype)

EMET Agent not protected by default

++

Future Work

- Applicable to many areas
- AppLocker / 3rd party application control software
- Firewall excluded paths / binaries
- Anti-Virus excluded paths / binaries
- Safer implant generation

++
Conclusions

+ MS Office deployments introduce many security holes, if not properly hardened
+ VBA is still remains a very reliable code execution container
+ Office Templates offer persistence opportunities in VDI implementations
+ Application control prevents the execution of external binaries but does block not native VBA code
+ WePWNise abuses configuration weaknesses to dynamically circumvent different defence layers
+ Disable VBA where possible! Plan carefully for exceptions

Previous Research / Credits / References

- Vincent Yiu (@vysecurity)
- Matt Nelson (@enigma0x3) https://enigma0x3.net/
- Casey Smith (@subtee) http://subt0x10.blogspot.co.uk/
- Didier Stevens (@DidierStevens) https://blog.didierstevens.com
- https://www.fireeye.com/blog/threat-research/2016/06/angler_exploit_kite.html
- https://www.microsoft.com/security/portal/enterprise/threatreports_july_2015.aspx#tab2
- https://blogs.technet.microsoft.com/srd/2016/02/02/enhanced-mitigation-experience-toolkit-emet-version-5-5-is-now-available
- https://technet.microsoft.com/en-us/itpro/windows/whats-new/device-guard-overview

< /dev/audience

- @mwrlabs

https://labs.mwrinfosecurity.com/

- Publishing code shortly