MWR Labs

++

One Template To Rule ‘Em All

Kostas Lintovois

28th October 2016

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

Macros recap

MWR LABS

++ Visual Basic for Applications (VBA)

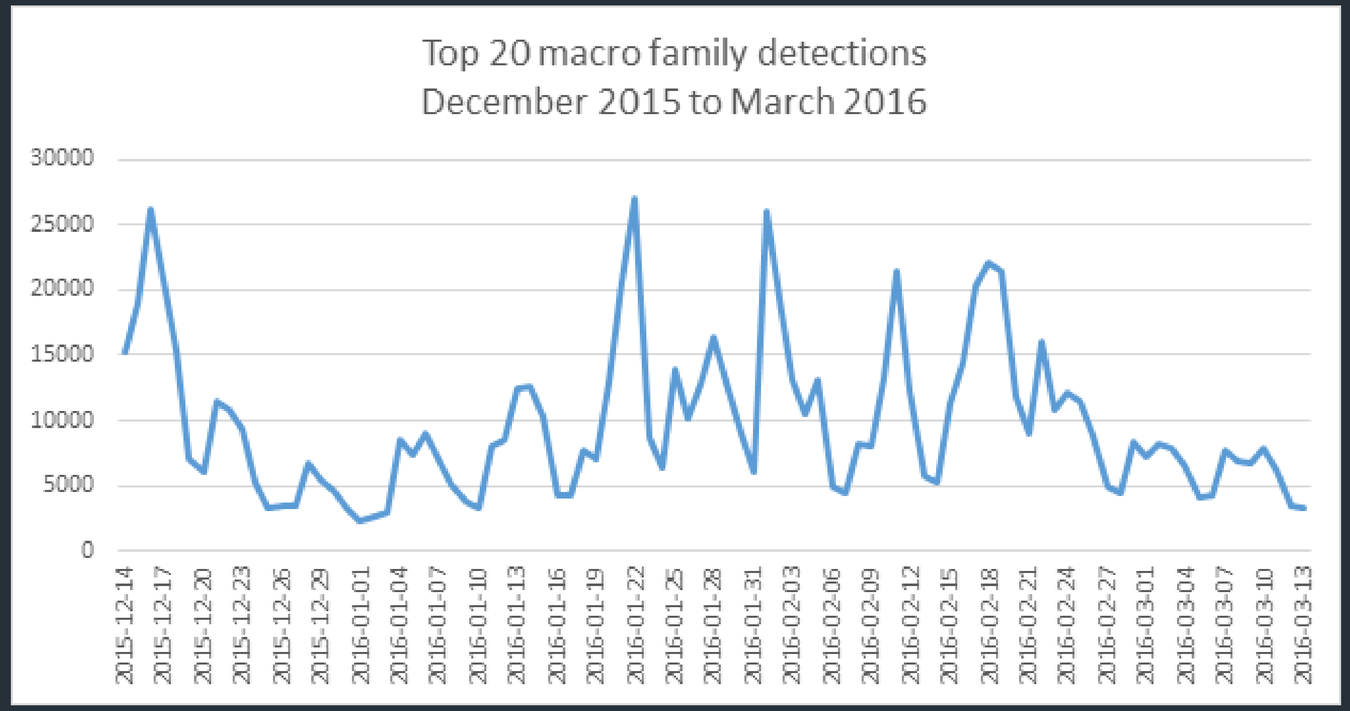
+ The VBA component is installed by default as part of Office's installation
+ VBA enables the use of multiple technologies
+ Office settings can be controlled locally or via GPO

Macros recap

MWR LABS

++ Visual Basic for Applications (VBA)

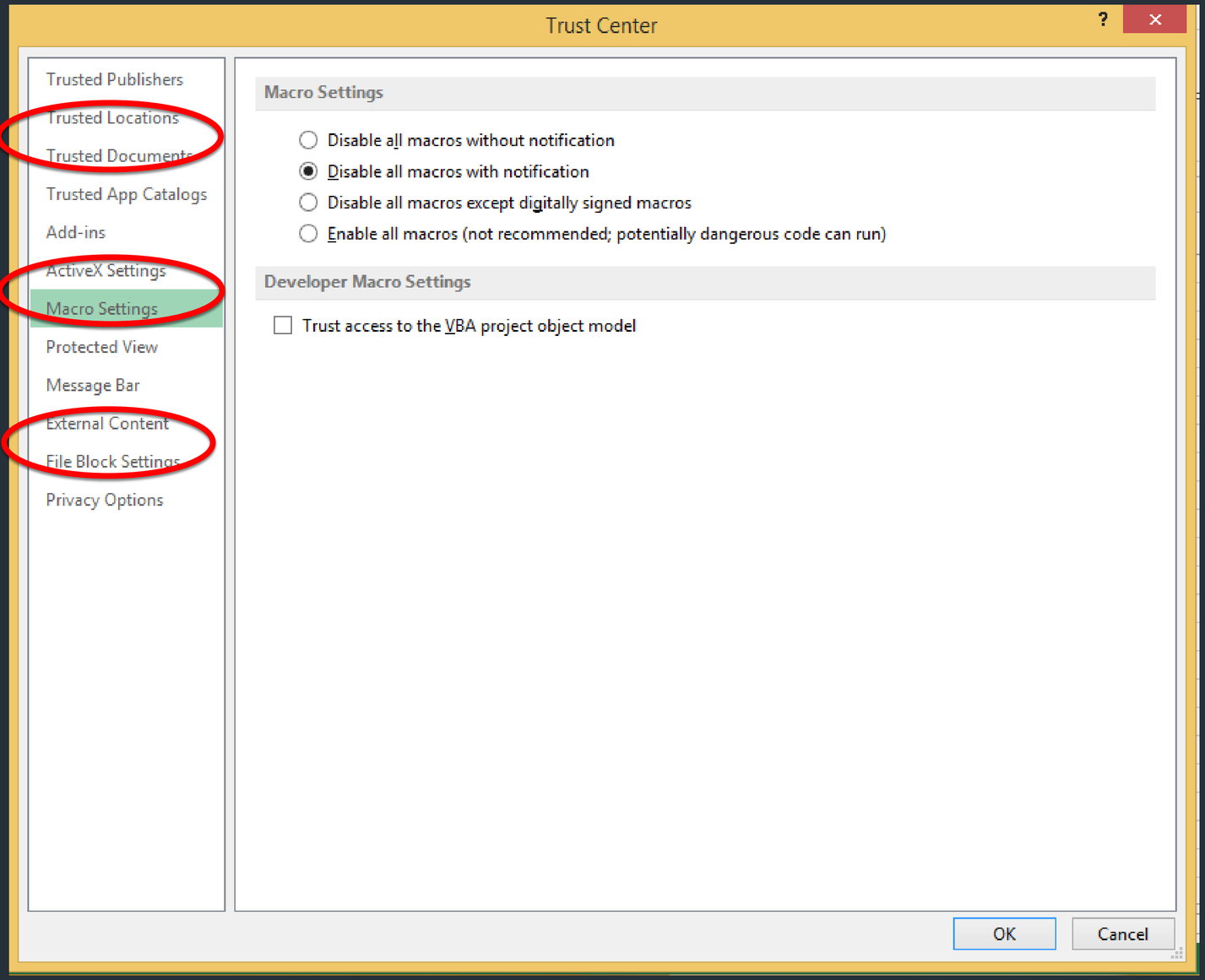
+ Macro-based malware infections are still increasing



Macros recap

++

Macros security settings



MWR LABS

++ Office settings via GPO

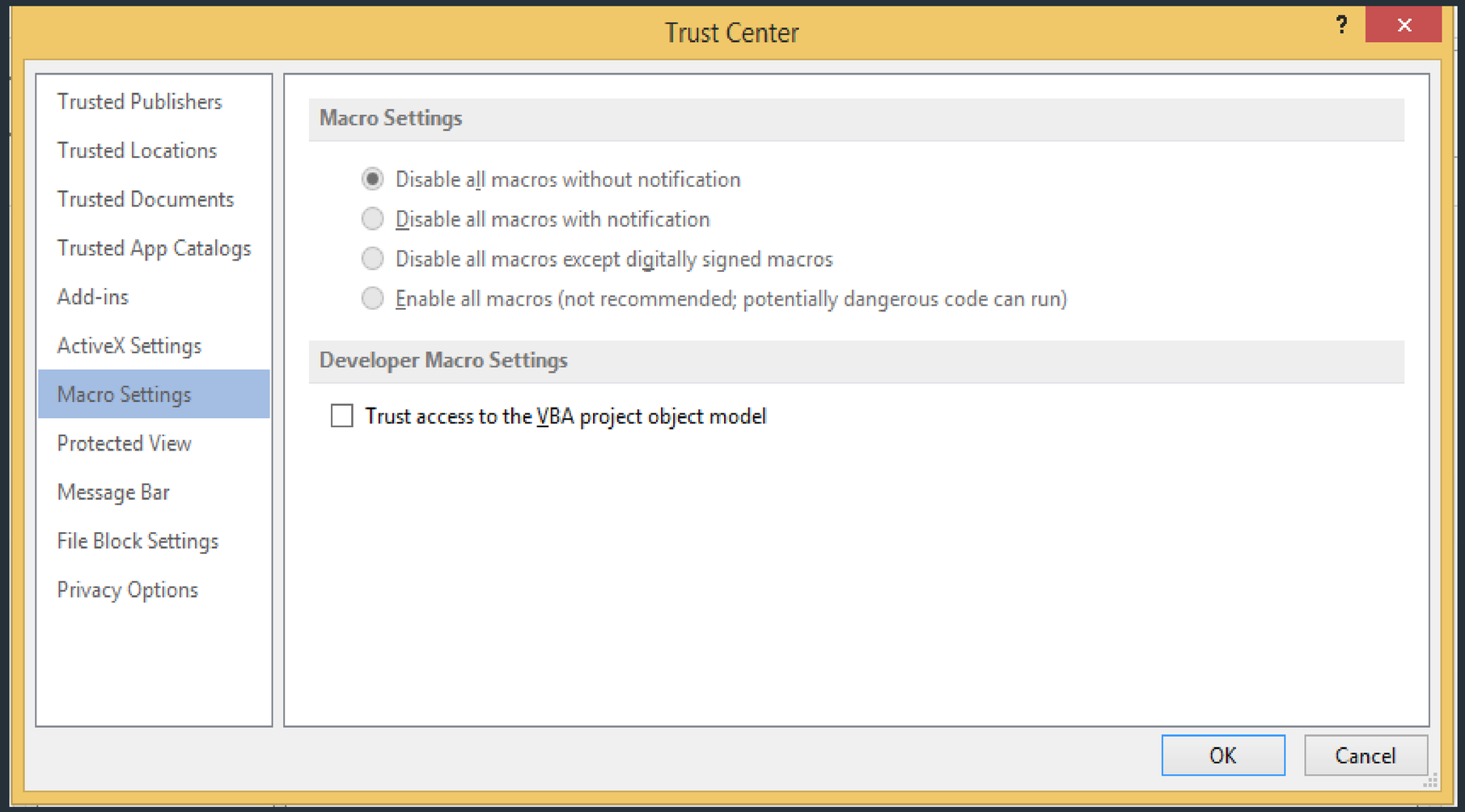
+ Every Office version ships with its own GPO Templates (ADMX/ADML)
+ Multiple settings within the GPO
  + Machine > Administrative Templates > Microsoft Office {version}
  + User > Administrative Templates > Microsoft Office {version} > Security Settings
  + User > Administrative Templates > AppName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

Macros recap

MWR LABS

++

Office settings via GPO



MWR LABS

++ Too many trusts

+ Trusted Locations
+ Trusted Documents
+ Trusted Publishers
+ Trusted App Catalogs

MWR LABS

++ 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

MWR LABS

++ Trusted Locations GPOs

+ Trusted locations can be controlled via GPO

+ Settings are defined within the user’s GPO branch

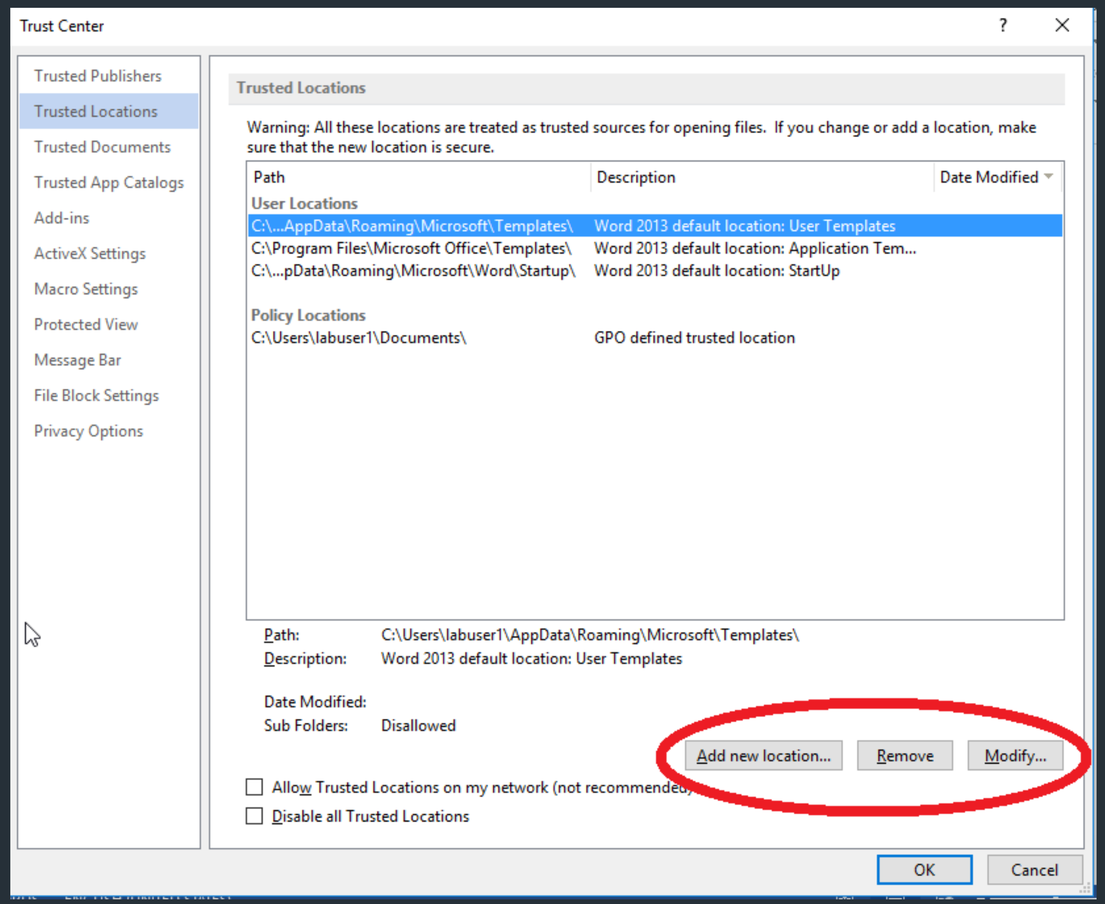
  + User > Administrative Templates > AppName {version} > AppName Options > Security Settings > Trust Center > Trusted Locations

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

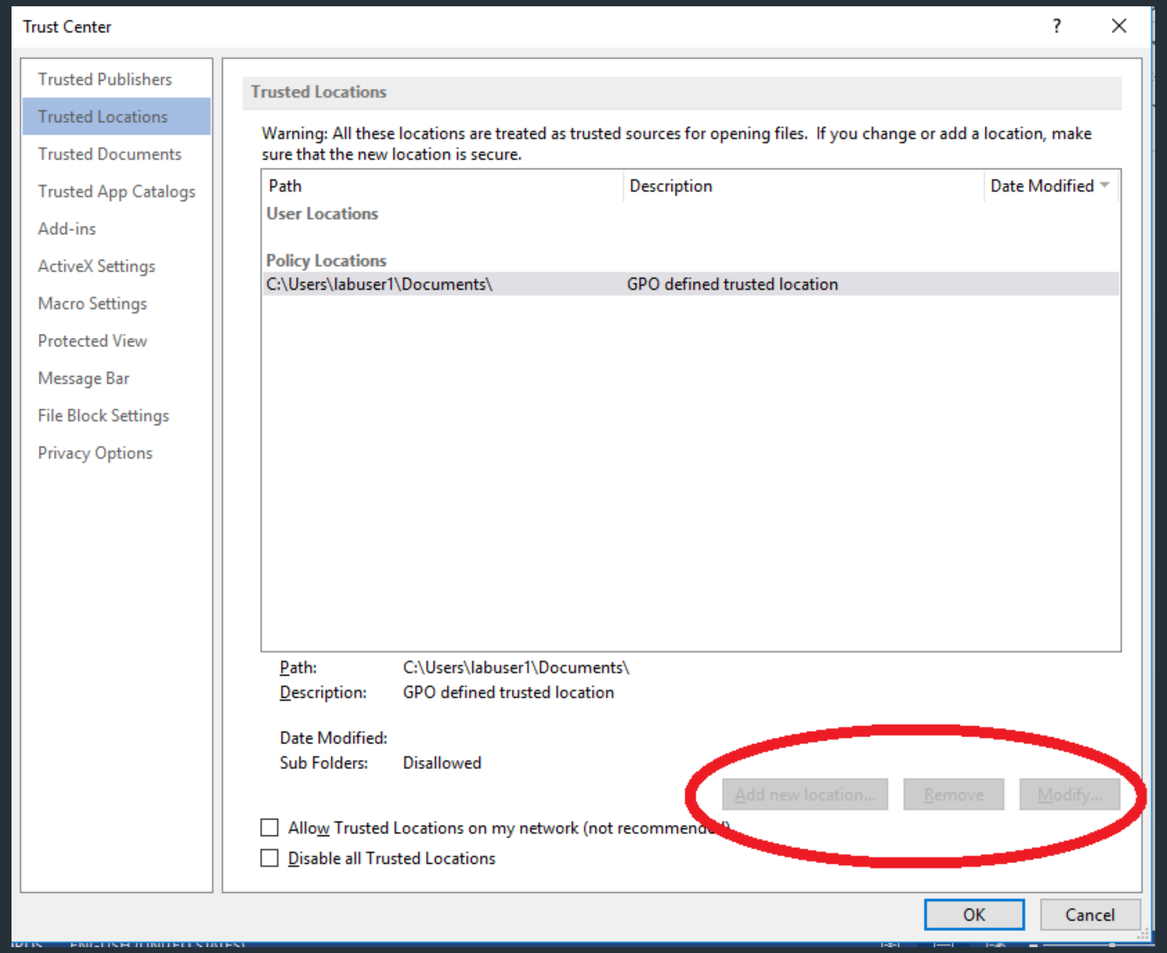
Office Trusts and Templates

++

Trusted Locations GPOs



VS



MWR LABS

++ 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

Office Trusts and Templates

MWR LABS

++ 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)

MWR LABS

++

Virtual Desktop Infrastructure (VDI)

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

MWR LABS

++ 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 ;)

MWR LABS

++ 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 ==

MWR LABS

++

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 ...)

MWR LABS

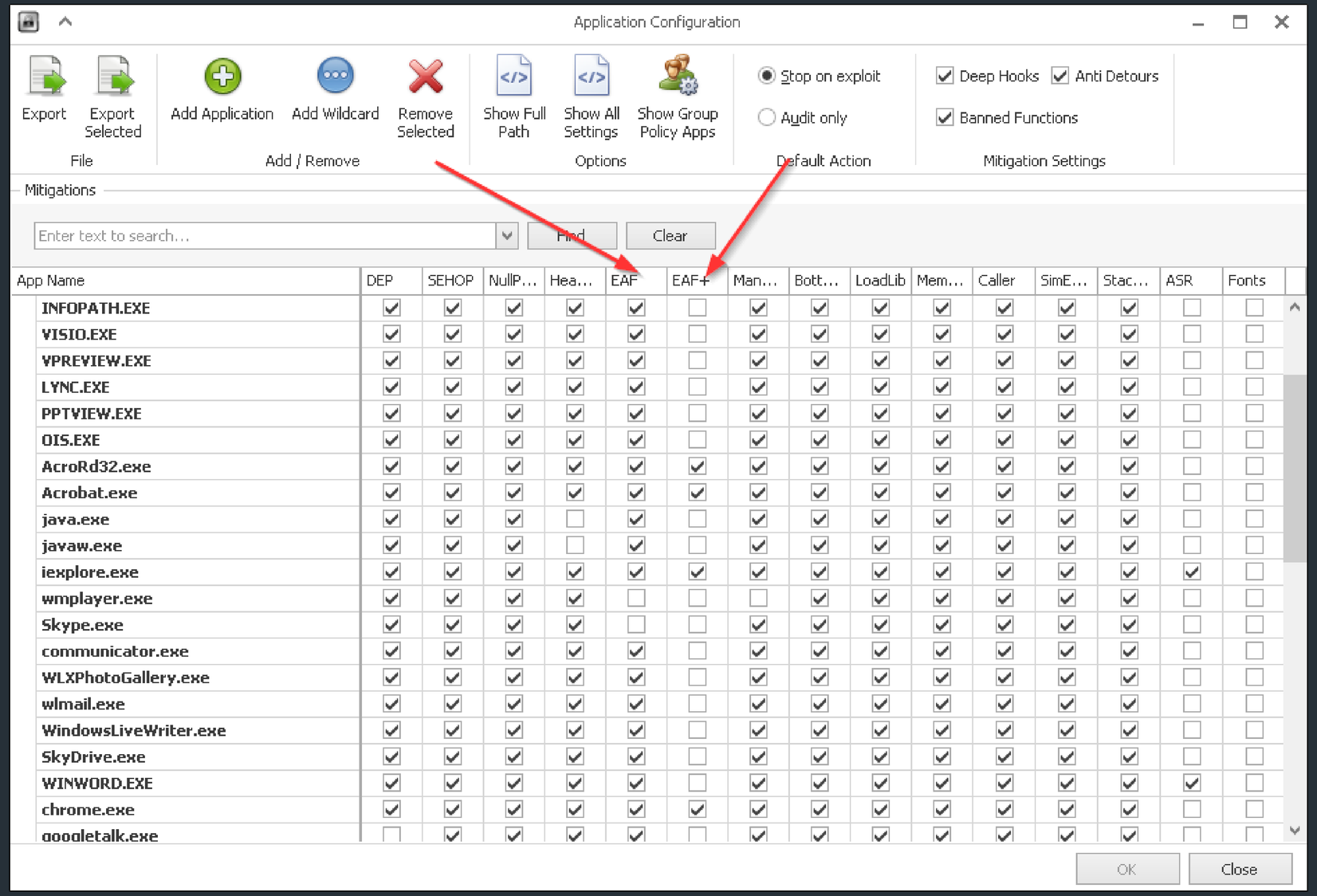
++ Raising the bar – EMET

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

what is EMET?

++

Raising the bar – EMET



MWR LABS

++ Current Macro Payloads (Metasploit)

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

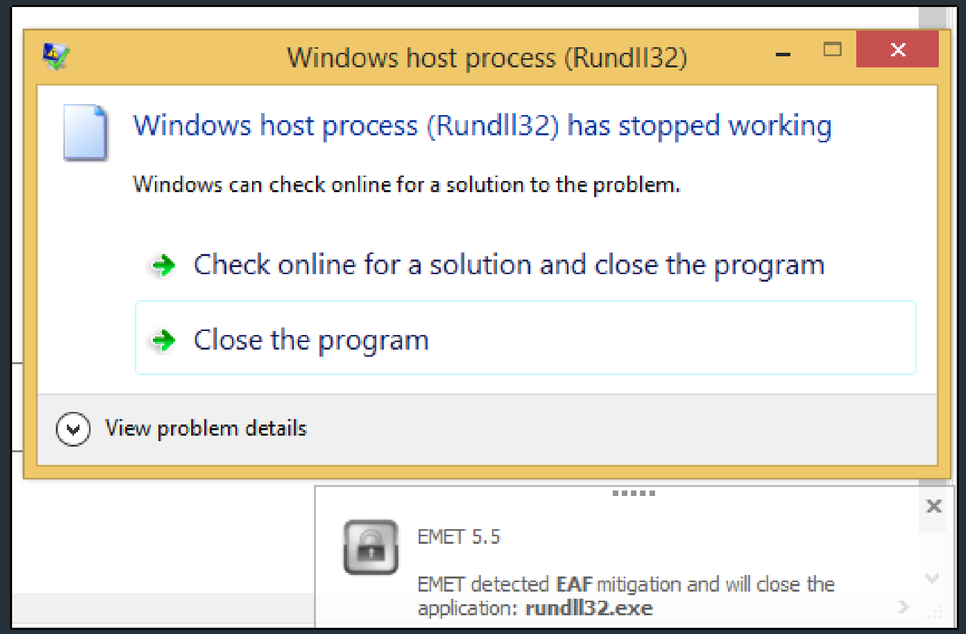
Existing Implants

MWR LABS

++ Current Macro Payloads (Cobalt Strike / Empire)

+ CS: Injects into Rundll32.exe

+ Empire: Wraps around powershell.exe



MWR LABS

++ Introducing WePWNise

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

MWR LABS

++ Configuration Weakness Exploitation

+ Enumerates Registry settings

+ Bypasses SRPs & EMET protected paths

+ Injection via WINAPI calls in VBA

MWR LABS

++ How does WePWNise inject?

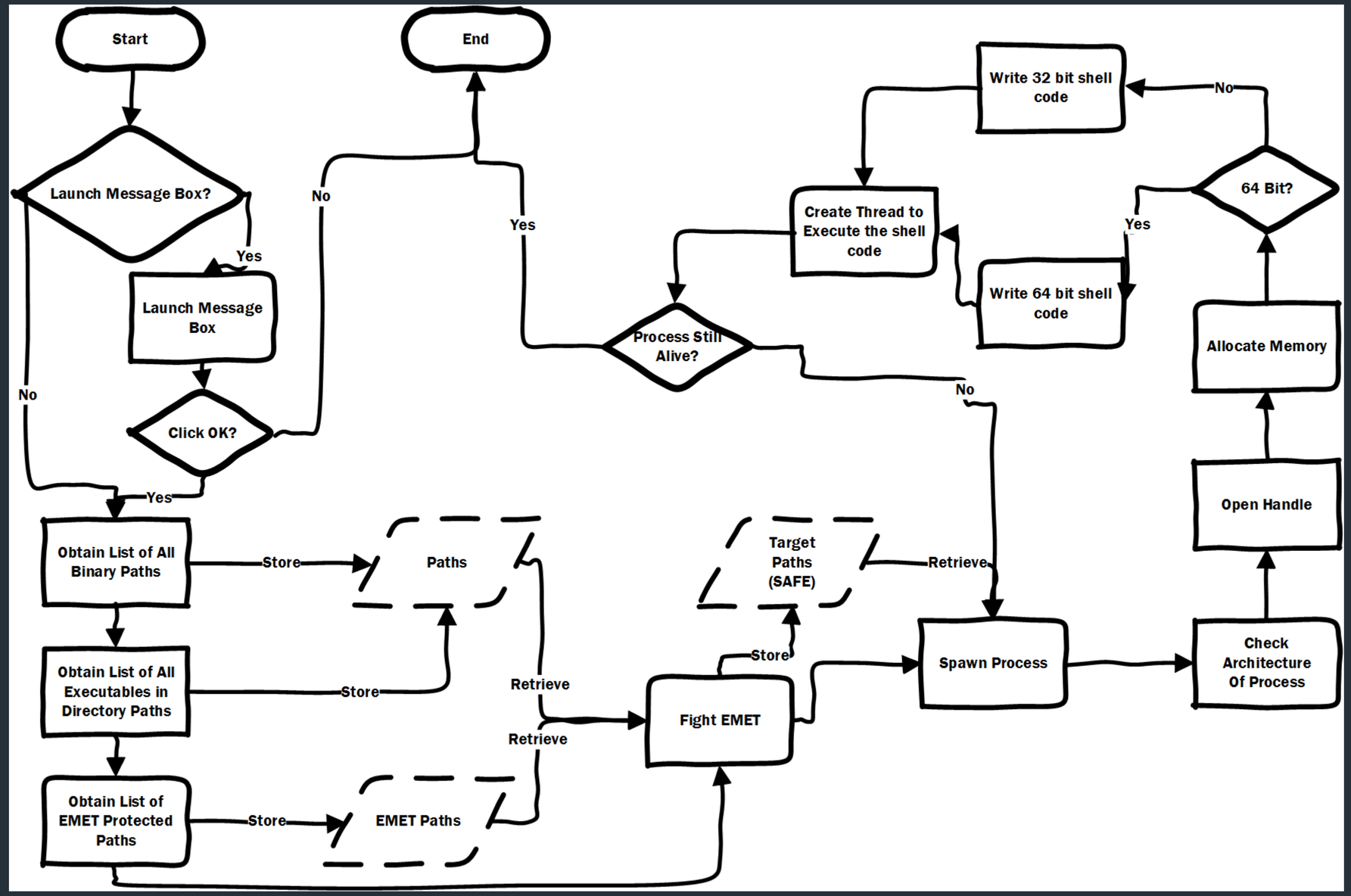
+ Native VBA code
+ CreateProcessA
+ VirtualAllocEx
+ WriteProcessMemory
+ CreateRemoteThread

WePWNise

++

WePWNise Map

MWR LABS



++ Enumeration

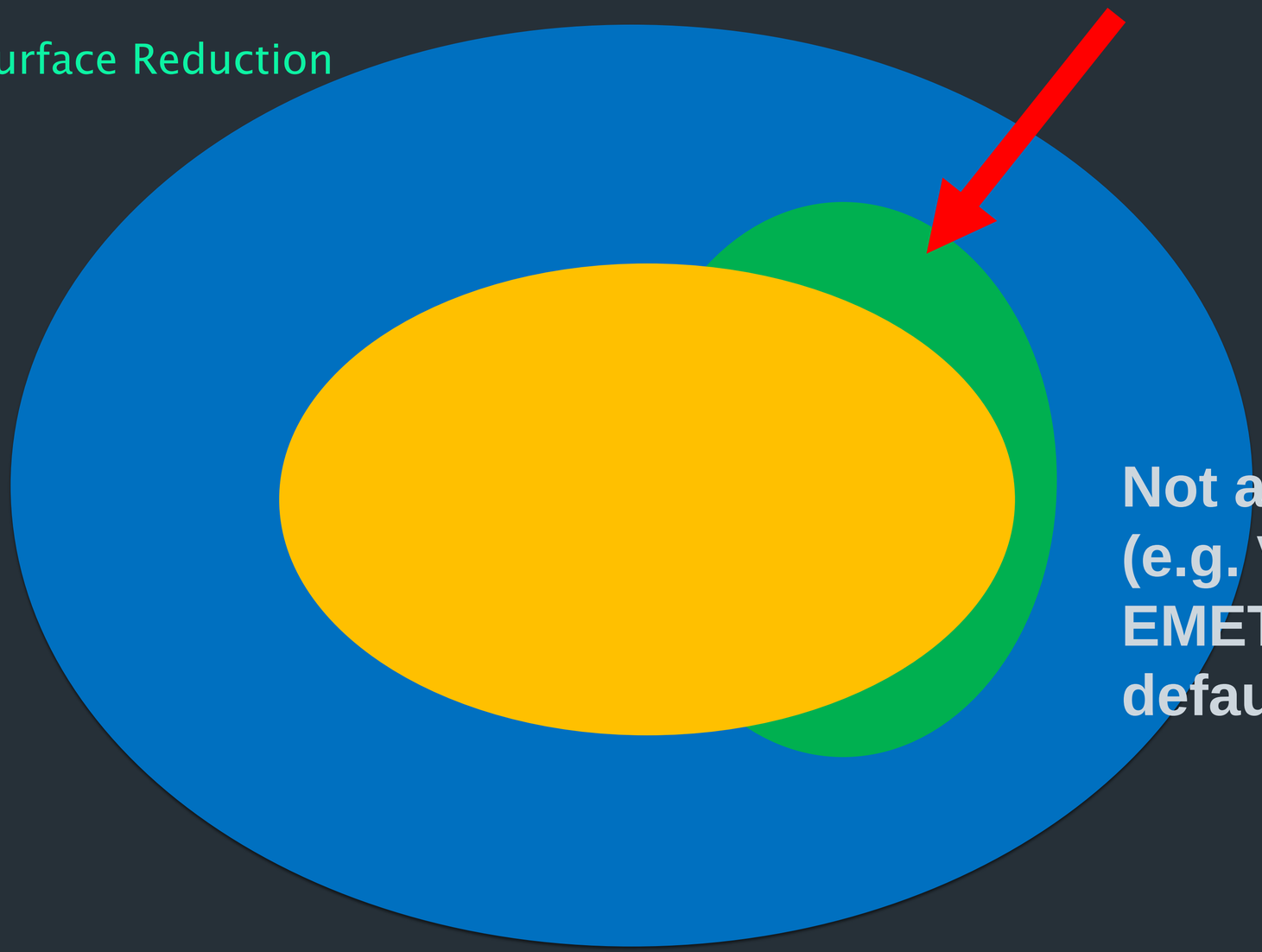
+ Native Registry Calls (Wscript.Shell)
+ HKLM\SOFTWARE\Microsoft\EMET\AppSettings
+ HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer
+ Metasploit:
  - > post/windows/gather/enum_emet
  - > post/windows/gather/enum_trusted_locations

WePWNise

++

Attack Surface Reduction

MWR LABS



All Binaries

Application Whitelist

EMET Protected

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

MWR LABS

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

MWR LABS

< /dev/audience

+ @mwrlabs

https://labs.mwrinfosecurity.com/

+ Publishing code shortly