

GP0 Vs Applocker Restrictions

Pralhad Chaskar (@c0d3xp10it)

What is GPO ?

- Group Policy, in part controls what users can and cannot do on a computer system: for example, to enforce a password complexity policy that prevents users from choosing an overly simple password, to allow or prevent unidentified users from remote computers to connect to a network share, to block access to the Windows Task Manager or to restrict access to certain folders.
- A set of such configurations is called a **Group Policy Object** (GPO).

GPO Settings

The screenshot shows the Local Group Policy Editor interface. The left pane displays a tree view of policy categories: Local Computer Policy > Computer Configuration > Software Settings, Windows Settings, Administrative Templates; and User Configuration > Software Settings, Windows Settings, Administrative Templates > Control Panel, Desktop, Network, Shared Folders, Start Menu and Taskbar, System, Windows Components, All Settings. The right pane is titled 'System' and lists various policy settings under the 'Setting' column. The 'Comment' column indicates that all listed items are set to 'Not configured' and have a value of 'No'. A 'Run' dialog box is overlaid at the bottom left, with 'gpedit.msc' typed into the 'Open:' field.

Setting	State	Comment
Ctrl+Alt+Del Options	Not configured	No
Driver Installation	Not configured	No
Folder Redirection	Not configured	No
Group Policy	Not configured	No
Internet Communication Management	Not configured	No
Locale Services	Not configured	No
Logon	Not configured	No
Mitigation Options	Not configured	No
Power Management	Not configured	No
Removable Storage Access	Not configured	No
Scripts	Not configured	No
User Profiles	Not configured	No
Download missing COM components	Not configured	No
Century interpretation for Year 2000	Not configured	No
Restrict these programs from being launched from Help	Not configured	No
Do not display the Getting Started welcome screen at logon	Not configured	No
Custom User Interface	Not configured	No
Prevent access to the command prompt	Not configured	No
Prevent access to registry editing tools	Not configured	No
Don't run specified Windows applications	Not configured	No
Run only specified Windows applications	Not configured	No
Windows Automatic Updates	Not configured	No

Today we cover below GPO Settings

- Prevent access to the command prompt
 - Blocking CMD.EXE
- Don't run specified Windows applications
 - Blocking POWERSHELL.EXE, POWERSHELL_ISE.EXE, MSBUILD.EXE, RUNDLL32.EXE, BGINFO.EXE, MSIEXEC.EXE, ATBROKER.EXE, TRACKER.EXE, INSTALLUTIL.EXE, CDB.EXE, REGSVR32.EXE, REGASM.EXE, CSC.EXE, ETC.

Prevent access to the command prompt

Prevent access to the command prompt

Comment:

Not Configured

Enabled

Disabled

Supported on: At least Windows 2000

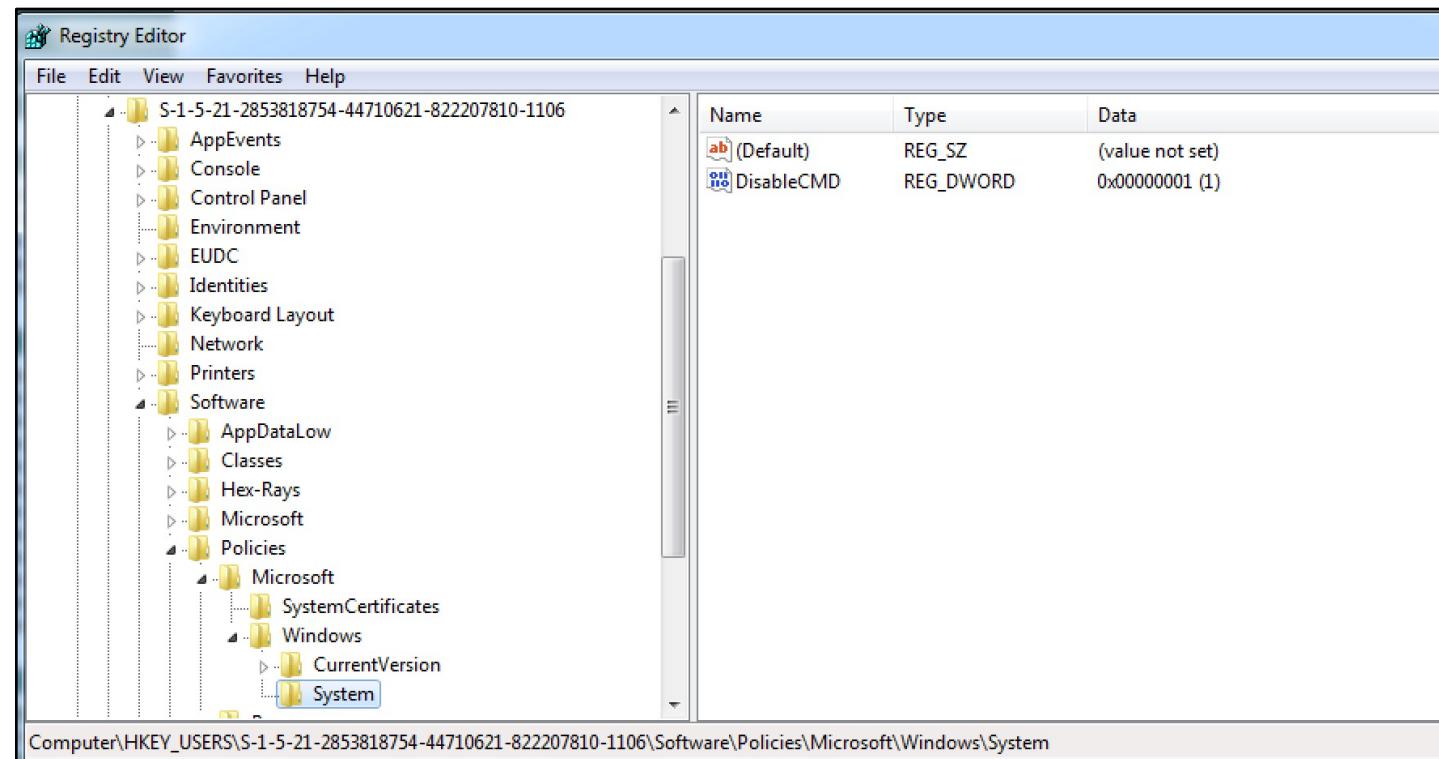
Options: Disable the command prompt script processing also? Yes

Help: This policy setting prevents users from running the interactive command prompt, Cmd.exe. This policy setting also determines whether batch files (.cmd and .bat) can run on the computer. If you enable this policy setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action. If you disable this policy setting or do not configure it, users can run Cmd.exe and batch files normally. Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Remote Desktop Services.

OK Cancel Apply

Registries added

- HKU\S-1-5-21-2853818754-44710621-822207810-1106\Software\Policies\Microsoft\Windows\System\DisableCMD: 0x00000001



Don't run specified Windows applications

Don't run specified Windows applications

Comment:

Enabled Comment:

Disabled Comment:

Supported on: At least Windows 2000

Options: Help:

List of disallowed applications

Show Contents

List of disallowed applications

	Value
▶	powershell.exe
	powershell_jse.exe
*	

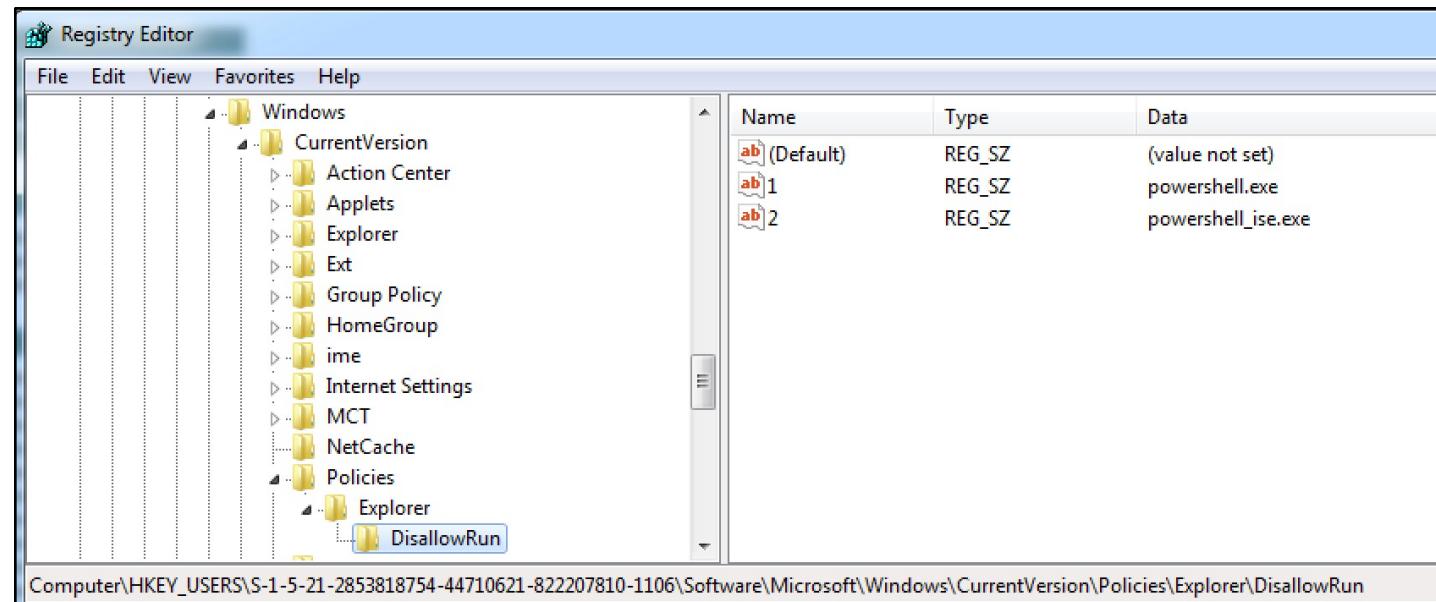
This policy setting only prevents users from running programs that are started by the File Explorer process. It does not prevent users from running programs, such as Task Manager, which are started by the system process or by other processes. Also, if users have access to the command prompt (Cmd.exe), this policy setting does not prevent them from starting programs in the command window even though they would be prevented from doing so using File Explorer.

Note: Non-Microsoft applications with Windows 2000 or later certification are required to comply with this policy setting.

Note: To create a list of allowed applications, click Show. In the

Registries added

- HKU\S-1-5-21-2853818754-44710621-822207810-1106\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun: 0x00000001
- HKU\S-1-5-21-2853818754-44710621-822207810-1106\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun\1: "powershell.exe"
- HKU\S-1-5-21-2853818754-44710621-822207810-1106\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun\2: "powershell_ise.exe"



Demo time!

Can above settings be bypassed ?



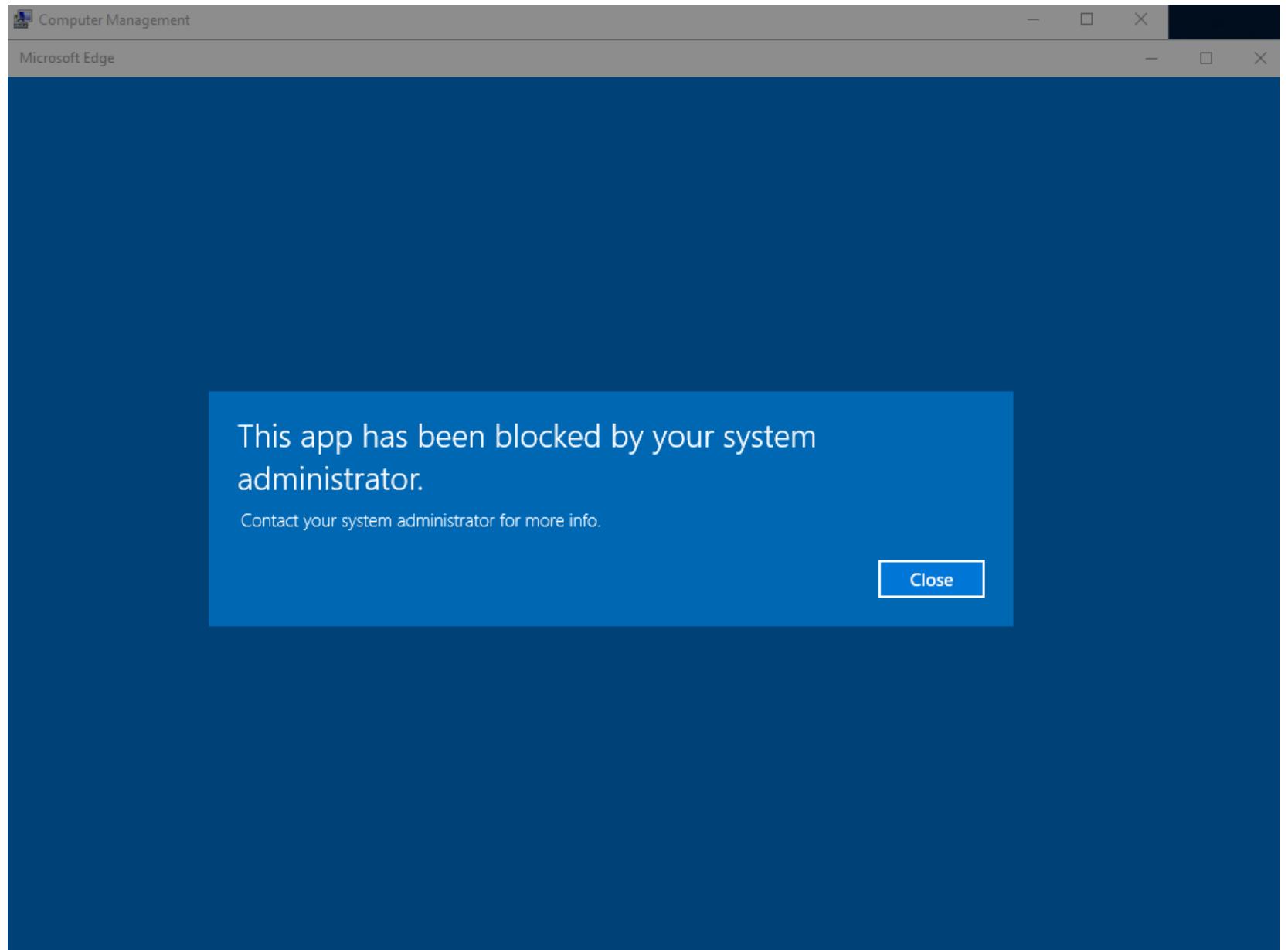
**YES
WE
CAN**

Demo time!

GPO Settings - Bypass

- Prevent access to the command prompt
 - Attacker can still access command prompt functions using ReactOS CMD.exe (Thank you Didier Stevens)
- Don't run specified Windows applications
 - Attacker can still access powershell.exe by calling through cmd.exe
 - Renaming powershell.exe and running from desktop

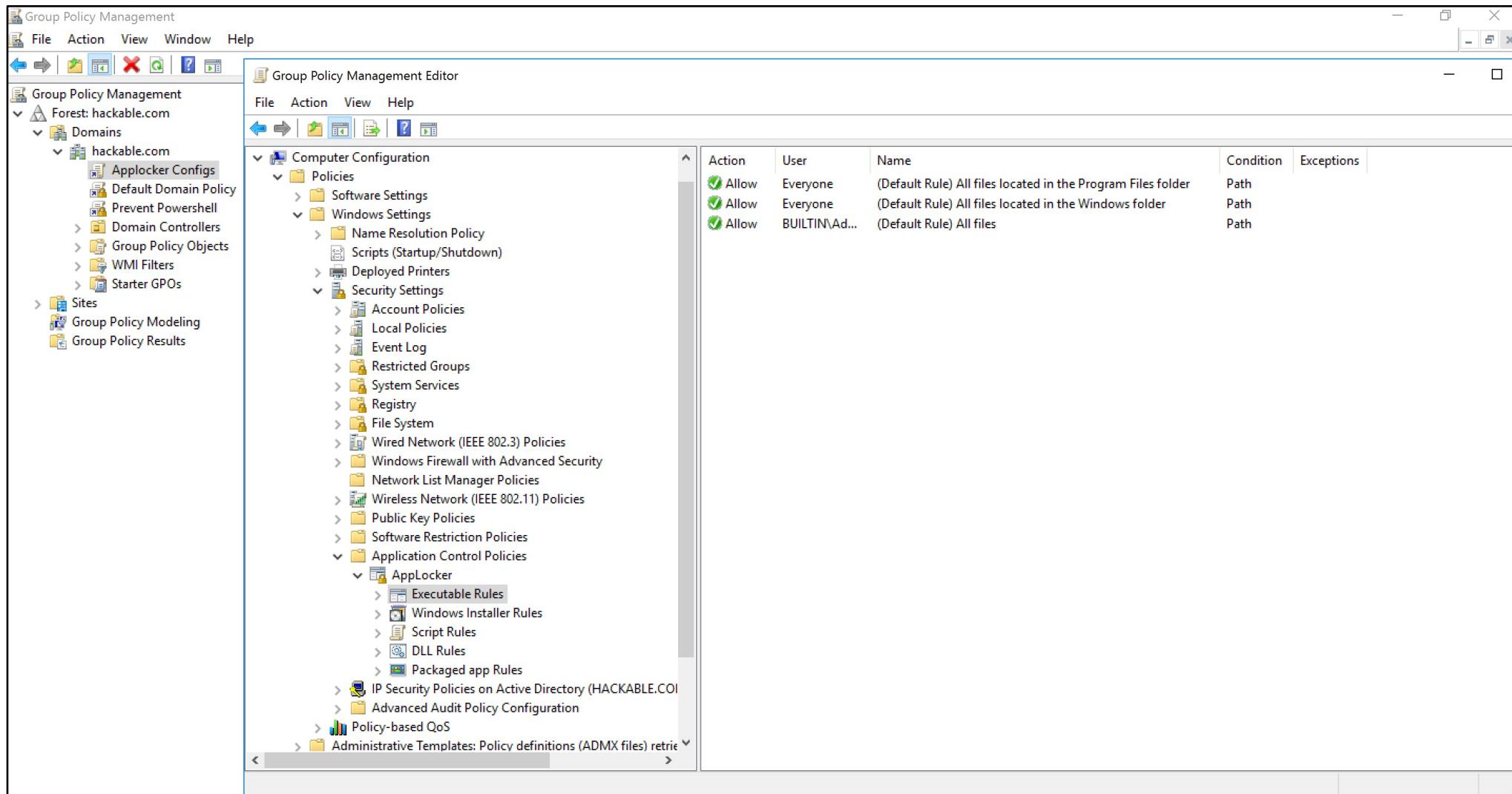
Applocker



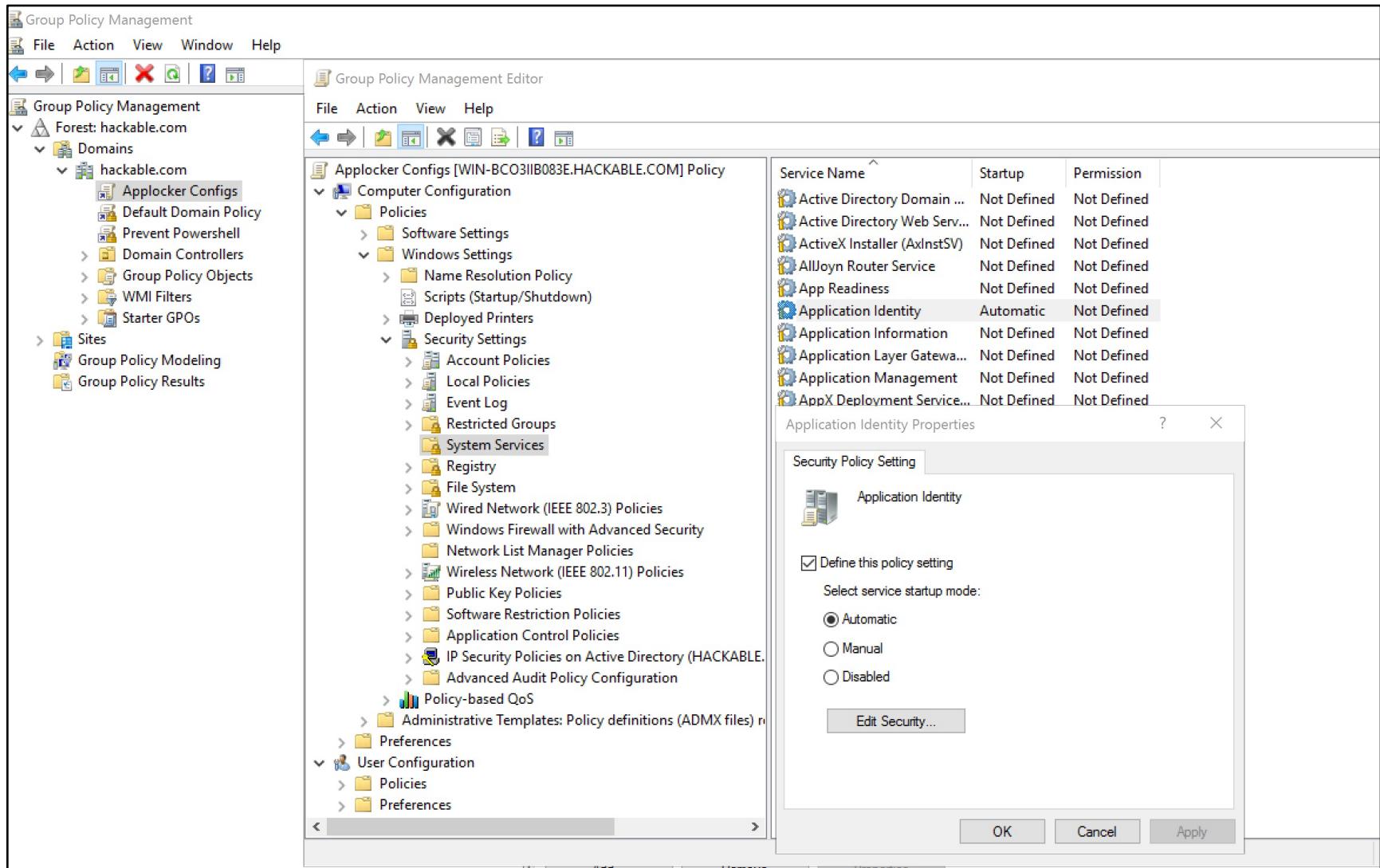
What is Applocker ?

- **AppLocker** is a new feature in Windows 7, Windows Server 2008 R2 and above that allows you to specify which users or groups can run particular applications in your organization based on unique identities of files. If you use AppLocker, you can create rules to allow or deny applications from running.

Configuring Applocker Default Rules



Service to be enabled



Lets see default rules block which binaries

- Below is sample list binaries that can be abused by attacker/adversary
 - Regsvr32.exe
 - Msbuild.exe
 - Rundll32.exe
 - Regsvcs.exe
 - Regasm.exe
 - Bginfo.exe
 - InstallUtil.exe
 - mshta.exe
 - IEExec.exe
 - cdb.exe
 - msieexec.exe
 - cmstp.exe
 - MavInject32.exe
 - odbcconf.exe
 -more other which we are unaware 😞

Rundll32.exe

- **Rundll32** is a Microsoft binary that can execute code that is inside a DLL file. Since this utility is part of the Windows operating system it can be used as a method in order to bypass AppLocker rules or Software Restriction Policies.
- So if the environment is not properly lockdown and users are permitted to use this binary then they can write their own DLL's and bypass any restrictions or execute malicious JavaScript code.

MSBuild.exe

- **MSBuild.exe** (Microsoft Build Engine) is a software build platform used by Visual Studio. It takes XML formatted project files that define requirements for building various platforms and configurations.
- Adversaries can use MSBuild to proxy execution of code through a trusted Windows utility. The inline task capability of MSBuild that was introduced in .NET version 4 allows for C# code to be inserted into the XML project file. MSBuild will compile and execute the inline task. MSBuild.exe is a signed Microsoft binary, so when it is used this way it can execute arbitrary code and bypass application whitelisting defenses that are configured to allow MSBuild.exe execution.

Lets run Rundll32.exe and MSBuild.exe
against default Applocker rules

Demo time!

MSBuild.exe bypassed default rules

Configuring Applocker to block MSBuild.exe

The screenshot shows the Group Policy Management Editor interface. On the left, the navigation pane displays a policy named "AppLocker Default [WIN-BC03IIB083E.HACKABLE.COM] Policy" under "Computer Configuration / Policies / Windows Settings / Security Settings / Application Control Policies / AppLocker / Executable Rules". On the right, a table lists the rules:

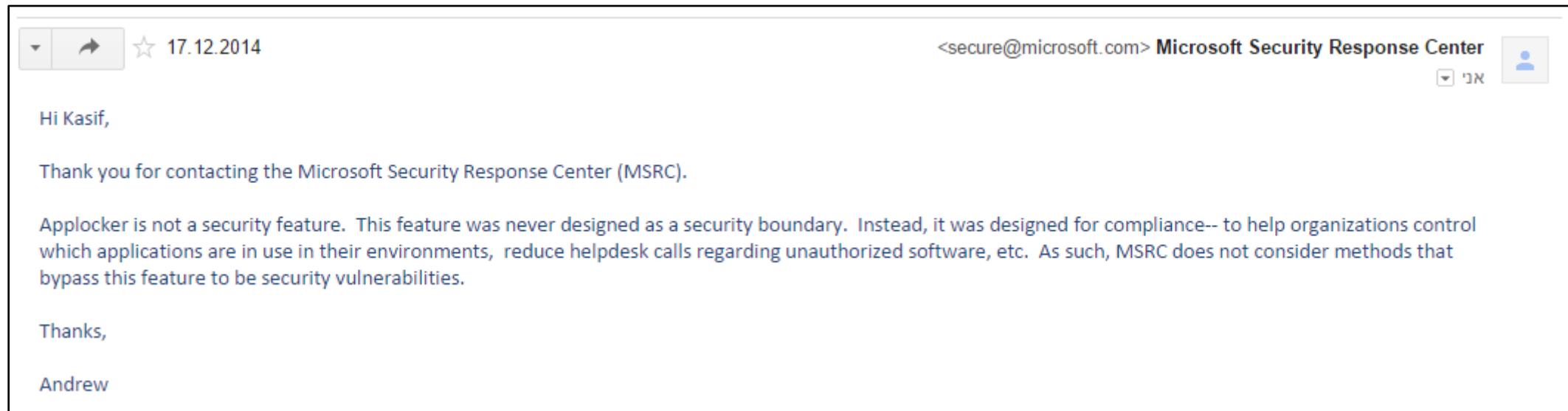
Action	User	Name	Condition	Exceptions
Allow	Everyone	(Default Rule) All files located in the Program Files folder	Path	
Allow	Everyone	(Default Rule) All files located in the Windows folder	Path	
Allow	BUILTIN\Administrators	(Default Rule) All files	Path	
Deny	Everyone	MSBUILD.EXE, in MICROSOFT® .NET FRAMEWORK, fr...	Publisher	

Demo time!

Summary

- Applocker is not a security feature
- Restrictions implemented by GPO are different from Applocker
- Review your defaults before implementing Applocker
- More research to follow this session....

Microsoft's Response to Applocker Bypasses



Reference :- <https://github.com/kasif-dekel/Microsoft-Applocker-Bypass>

Information security is always an arms race !!



References

- <https://oddvar.moe/>
- <https://pentest.blog>
- <https://github.com/redcanaryco/atomic-red-team>



THANK
YOU FOR
LISTENING
ANY
QUESTIONS?