

AppLocker Bypass – CreateRestrictedToken

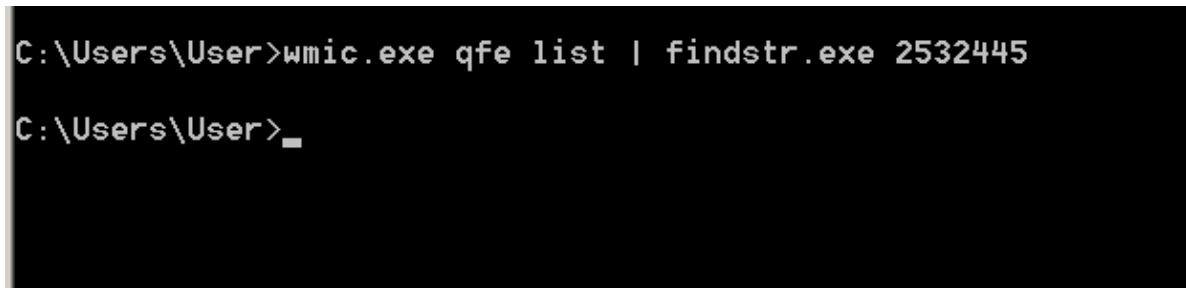
pentestlab.blog/category/red-team/page/101

July 7, 2017

Bypassing AppLocker most of the times it's a matter of trusted Microsoft binaries that can execute code or misconfigured policies that could be easily exploited. However it is possible to bypass SPR or AppLocker by exploiting an architectural design. Specifically in Windows 7 and Windows 2008 Server environments it is possible to abuse an API function (CreateRestrictedToken) to achieve the bypass. Microsoft has released a [patch](#) to address this issue.

Identification of the missing patch can be done easily from the command prompt:

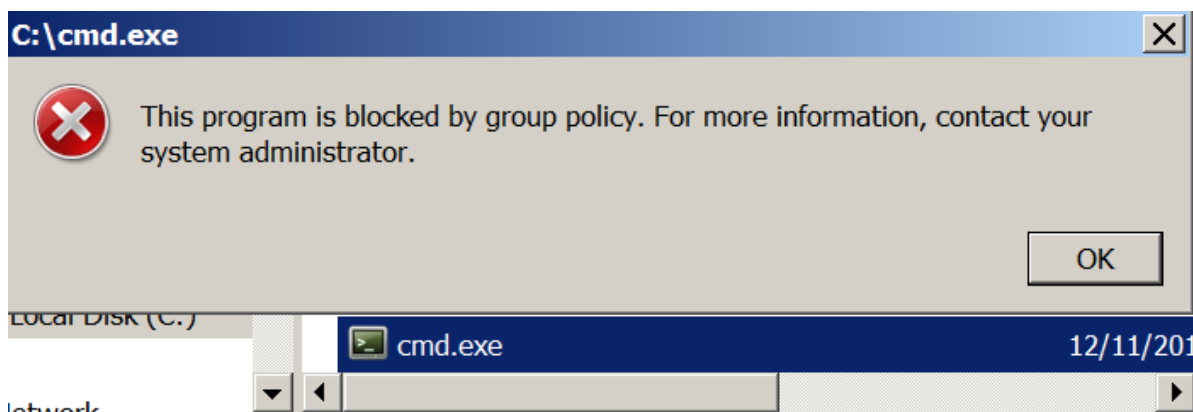
```
wmic.exe qfe list | findstr.exe 2532445
```



```
C:\Users\User>wmic.exe qfe list | findstr.exe 2532445  
C:\Users\User>_
```

AppLocker Patch is Missing

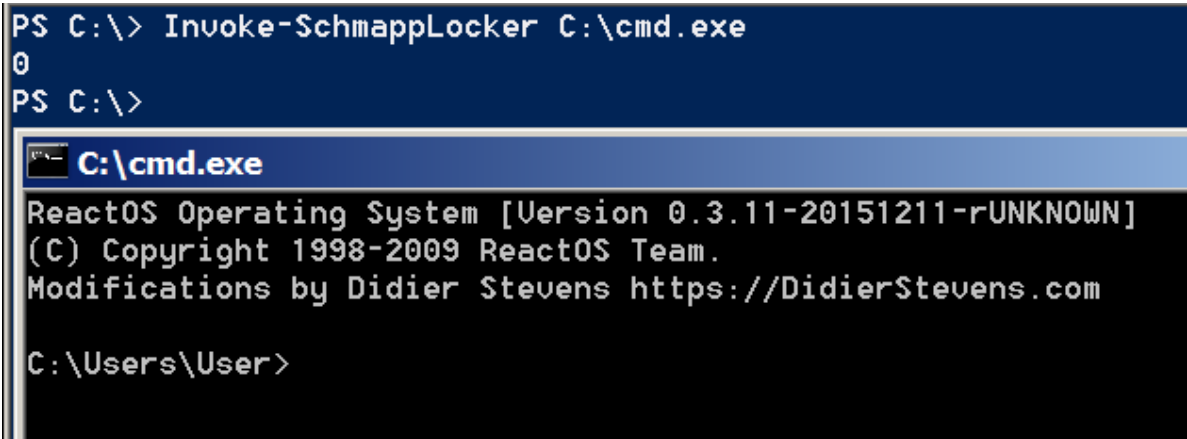
Since there is no output this indicates that the KB2532445 patch is missing. Trying to execute an untrusted binary directly it will fail due to AppLocker restrictions.



Executing an untrusted binary

There is a PowerShell [script](#) developed by [Michael Bailey](#) which exploits the API function **CreateRestrictedToken** by using the **SANDBOX_INERT** flag in order to allow execution of binaries. Since this flag disables checks for all rule collections it is possible to bypass AppLocker and Software Restriction Policies. This vulnerability was discovered originally by [Didier Stevens](#) and it was fully documented in his [blog](#).

```
PS C:\> Invoke-SchmappLocker C:\cmd.exe
0
PS C:\>
```



AppLocker Bypass – CreateRestrictedToken

References

[Circumventing SRP and AppLocker to Create a New Process, By Design](#)

<https://support.microsoft.com/en-us/help/2532445/you-can-circumvent-applocker-rules-by-using-an-office-macro-on-a-compu>

<http://baileysoriginalirishtech.blogspot.co.uk/2015/06/applocker-schmapplocker.html>

<https://github.com/strictlymike/Invoke-SchmappLocker/blob/master/Invoke-SchmappLocker.ps1>