CERT-In

Indian Computer Emergency Response Team

Enhancing Cyber Security in India

Botnet: An Overview

By

Basudev Saha and Ashish Gairola

Department of Information Technology
Ministry of Communications and Information Technology
Govt. of India

Issue Date: June 17, 2005

Index

1. Introduction 3
2. Propagation Mechanism 3
3. Bot nets 4
3.1. IRC bots 5
3.2. Botnet in numbers 6
4. Botnet Malicious activities 6
5. Countermeasures 7
6. Reference 7
Annexure I - Analysis of a bot 8
Annexure II- Desktop defense reference 12

1. Introduction

The term Bot is derived from the word “Robot”. Robot comes from the Czech word "robot," which means "worker". In computer world Bot is a generic term used to describe an automated process.

Bots are being used widely on the Internet for various purposes. Bot functionality may vary from search engines to game bots and IRC channel bots. Google bot is one such famous search bot, which crawls through the web pages on the net to collect information and build database to enable variety of searches. Computer controlled opponents and enemies in multiple player video games are also a kind of bot, where the computer process tries to emulate the human behavior.

However, the usage of bots is not limited to good purpose only. Bots are widely used to perform malicious activities ranging from information stealing to using as a launching pad for distributed attack. Such software’s gets installed on user computer without their knowledge. Some bot infected machines, pass the control of the machine to a remote attacker and act as per the attackers command. Such machines are popularly known as zombie machines.

2. Propagation Mechanism

An attacker may adopt any of the following techniques or a combination of the techniques for wide distribution of a particular bots.

Web/Mail Download -

Various websites knowingly or unknowingly host malicious contents and infect the client machines visiting those sites. Attaching malicious software along with innocent looking mails is a popular means of spreading malware. Mass mailing techniques (Spam) simplify and enable fast spreading of such malware easily.

Installing software from un-trusted sources

Installing free utility software from un-trusted or unknown sources may also bring malicious content to the user’s computer. It is observed that some peer-to-peer network client software comes bundled with adware or spyware.

Scan exploit and plant

In the first two methods of propagation active user intervention is required. However, there are techniques for automated distribution of these malware without the need of active user intervention. Malicious contents like trojans, bots etc are planted to end users computer by exploiting known vulnerabilities in a computer system. Mass scanning for finding computers with known vulnerabilities is either done manually by an attacker, or it can be orchestrated by automated self spreading worms and viruses. CodeRed, Mydoom, Sql Slammer are some of such self spreading worms, which scan the network for machines with a particular vulnerability, exploit them and plant themselves in the affected computers. Worms like MyDoom open a backdoor to be exploited by hackers later on. Such automated worms primarily target flaws with Microsoft windows machines. A recent study by German Honeynet Project [Ref 1] shows that most of the traffic targets the port used for resource sharing in Windows operating system, namely port 445/TCP (Microsoft-DS Service), 139/TCP (NetBIOS Session Service), 137/UDP (NetBIOS Name Service), 135/TCP (RPC Services). Majority of the Internet noise are caused by these automated activities.

3. Bot nets

Botnets are network of compromised machines under the control of attackers. These machines can be used by attackers to launch attacks or to engage in various other kinds of malicious activities. Bot infected machines opens a backdoor and listen for commands issued by attackers. For controlling and issuing commands to a large number of bots at a time an attacker adopts various kinds of controlling mechanisms. Popular media for controlling botnets are IRC channel and P2P network. In this document our discussion will primarily focus on IRC bots.

IRC basics

Internet relay chat is a popular chatting system. It is defined in rfc1459. IRC is based on client-server model. IRC Servers enable communications between clients using IRC protocol. They are run by various organizations. Some of the popular IRC networks are darknet.org, cyberarmy.net etc

IRC clients are used at the user end to log on to IRC server network, and to communicate with other logged in users through the IRC servers. Some of the popular IRC clients are MIRC, IRC etc.

IRC though works on generic client server architecture; it also allows clients to establish connection between them for direct communication. The communications between bots and IRC servers by default takes place in plain text; however, there are ways of encrypting the communication between them.

Channels

Channels are virtual meeting place for a group of users using the same IRC server or network. They can be created by any user. Channels exist as long as at least one user is logged in into that channel. Channels are controlled by channel operator. The channel operator can restrict the usage of the IRC channel. Channels are named as #channel_name.

Nickname

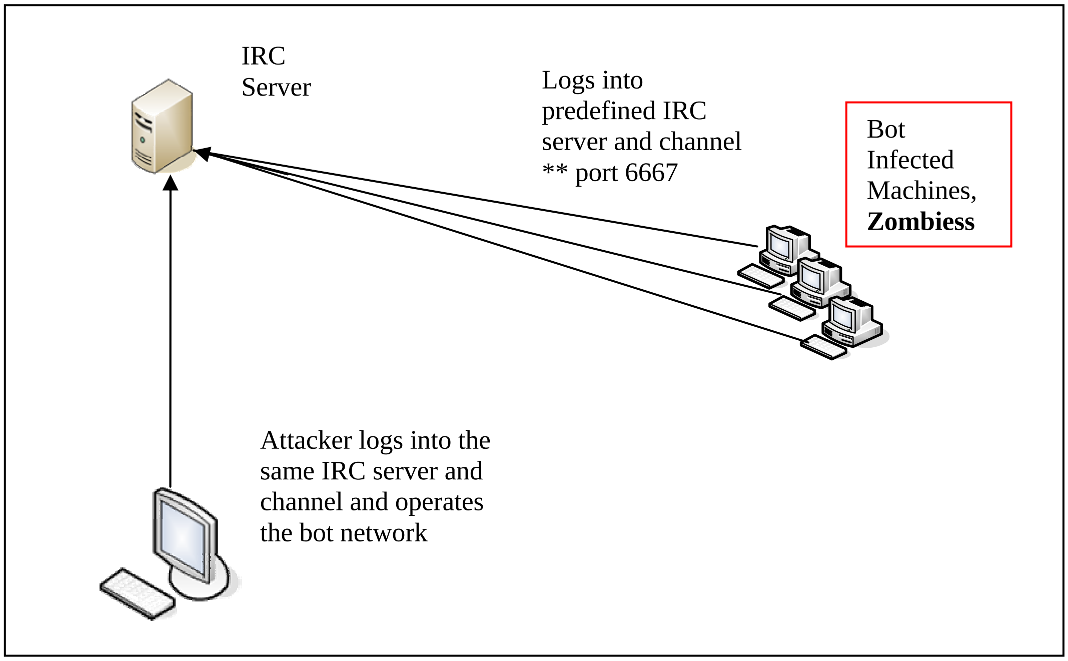
Nickname is the identification name of the logged in user. However, unlike other popular chatting system like yahoo and MSN, most of the IRC server does not employ any authentication or registration mechanism for using their services.

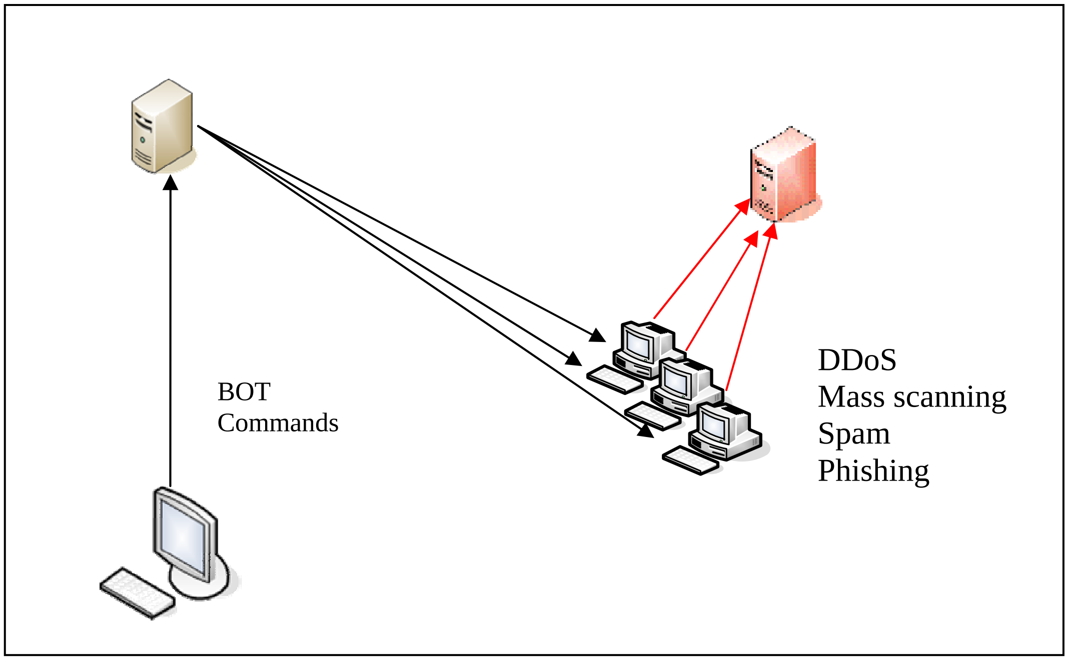
Bots

Since the inception of IRC networks, Bots are widely used for various good purposes. Primarily it is being used as a channel operator for administrating channels in an automated fashion. Eggdrop, winbot are some of such good bots being used in the IRC networks widely.

3.1. IRC bots

IRC networks are a popular medium for controlling bot networks. An IRC bot, when executed in a client machine, connects to IRC server (generally on port 6667), and logs in to a specific predefined channel and listens for commands issued by master controller. The attacker or bot net controller acts as the operator for that particular channel and issues commands to the bots. Commands with specific syntax issued in that particular channel, are executed on all the bot infected machines that are currently logged in the channel. Some of the famous and widely used IRC bots are Agobot, GTBot, SDBot, Evilbot etc. A detailed analysis of a sample bot is given in Annexure I.





3.2. Botnet in numbers

A bot network can contain thousands of bot infected machines. These networks can be used to launch major attacks bringing down corporate networks or even national internet backbones. A recent study by honeynet.org had revealed a single bot network containing 50,000 infected machines [Ref 2]. Considering that each machine having an uploading bandwidth of 50kbps (a dial up connection), a network of 50,000 machines can generate traffic of ~300 MB per second. This is enormous enough to choke major corporate Internet bandwidths. Study by honeynet.org revealed that Phatbot alone had infected more than 400,000 machines.

4. Botnet Malicious activities

Internet users face botnet threats on two fronts: Getting infected by bots and being used for malicious purposes i.e. unknowingly the bot affected computer owners are becoming source of attack. On the other side corporate and end users may fall victim to coordinated targeted attacks from botnets, such as DDoS.

Bots like GTBots (Global Threat bots) are designed with wide range of features and they can be customized as per the requirement of the bot controller. Modules for specific attacks can be downloaded to the bot infected machine by an attacker to perform specific tasks like web site hosting, scanning, spam engine etc.

Denial of service attack –

DDoS attacks are the most common attacks performed by Botnets. The attack may be done by flooding large ICMP packets or SYN packets to the targeted network, or just sending thousands of legitimate http, ftp requests to the site.

Phishing

Bots are also effectively used for hosting phishing sites, making it extremely difficult for financial organizations to track such fraudulent sites.

Spam

Spam bots come along with an SMTP engine and they can send spam on attacker’s will. Phatbot is one such bot widely being used for spamming.

According to e-mail security service provider MessageLabs, nearly 70 percent of all spam and phishing e-mails now originate from botnets.

Spreading of new malware

Using bot network for spreading malicious codes are also observed in the wild. Such bot machines search the internet for machines with specific vulnerability, exploit them and plant malicious codes on that.

Apart from the above mentioned malicious activities, bots may also be engaged in other local attacks as an adware or spyware. These include information stealing, key logging, sniffing or popping up ads etc. These bots generally transmit information back to a third party without notifying the user, monitor and profile user’s web usage and direct pop up ads based on user’s surfing habits. More dangerous spywares may even act as a key logger and start passing every key pressed by a user, revealing user's secret information like credit card info, password etc.

5. Countermeasures

Home user

- Use updated antivirus, and anti-spyware software. Source for various antivirus and antispyware is given for reference [Annexure II].
- Use updated operating system and apply latest patches released by vendor
- Use local firewall. Keep a check on firewall logs and alerts.
- Disable active scripting execution features of browsers.
- Report unusual behavior
- Avoid visiting suspicious sites.
- Avoid opening suspicious mail attachments.
- Avoid installing software from un-trusted sources.

Corporate

- Corporates should have adequate desktop defense mechanism along with proper perimeter defense in place.
- Corporates networks should block outgoing connections to port 6667, if IRC communication is not required.
- IDS and IPS systems should be monitored regularly to detect anomalies in traffic pattern.

6. Reference

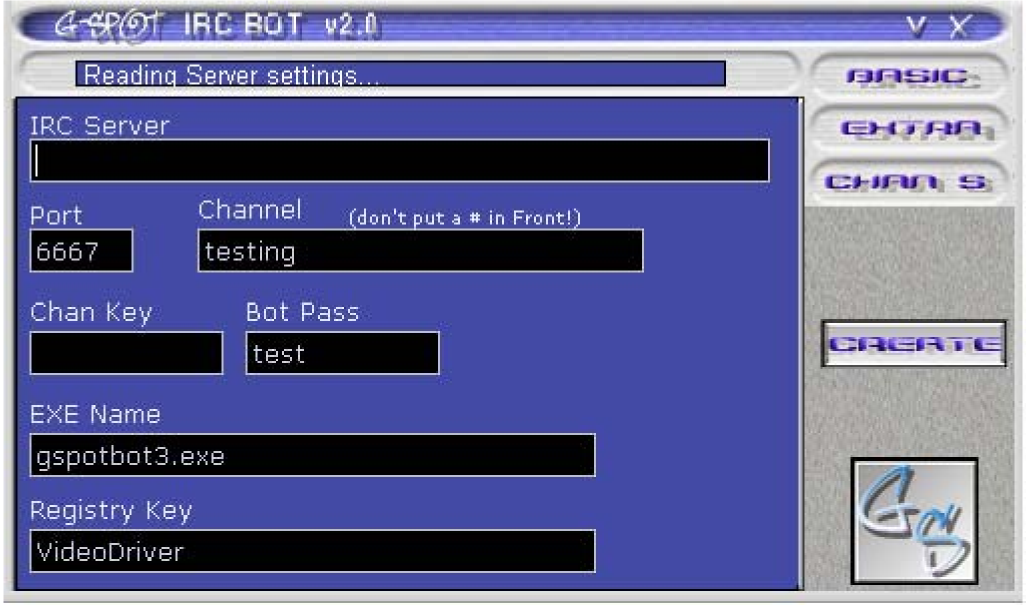
1. http://www.honeynet.org/papers/bots/
2. http://www.ietf.org/rfc/rfc1459.txt
3. http://www-i4.informatik.rwth-aachen.de/lufg/honeynet

Annexure I - Analysis of a bot

To have a better understanding of working of bot nets and their functionality, an analysis of a malicious bots were done in lab environment. This particular analysis is being done with a bot known as “g-spot bot”. The malicious binary files were available in the internet and were downloaded for test purpose.

The complete life cycle of the botnet follows as –

- Customizing the bot executables to login to a predefined IRC network and channel.
- Distributing the customized bot executable through various propagation mechanisms as discussed earlier.



Reading Server settings...

IRC Server

Port
6667

Channel (don't put a # in Front!)
testing

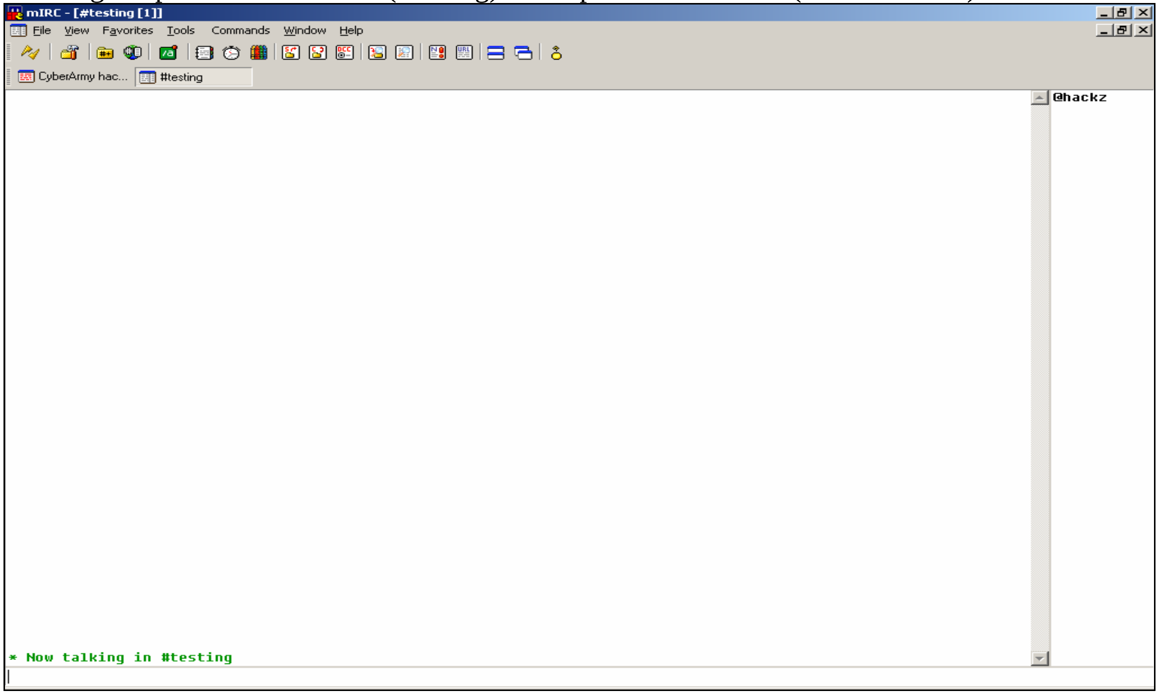
Chan Key

Bot Pass
test

EXE Name
gspotbot3.exe

Registry Key
VideoDriver

Creating the predefined channel (#testing) in the predefined server (IRC. ….. .net)

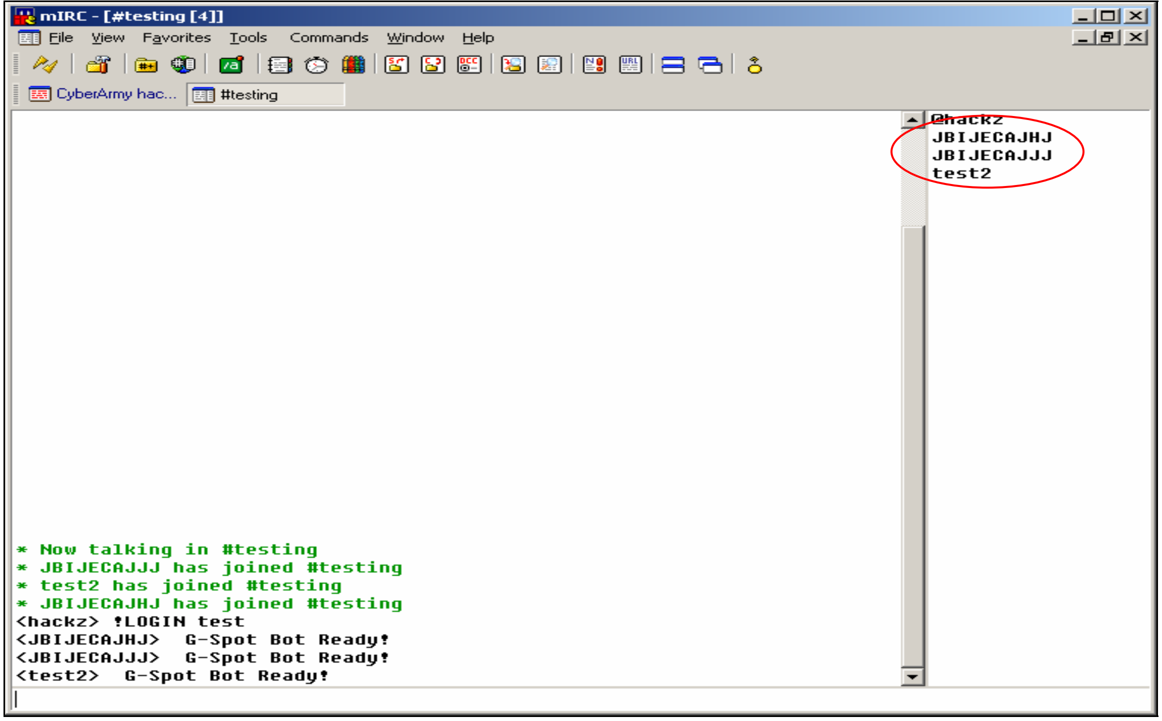


```
* Now talking in #testing
```

```
@hackz
```

On execution of the binary at the users side, the users machine logs in into the predefined channel and waits for command issued in that channel. Thus it becomes part of the bot-network.

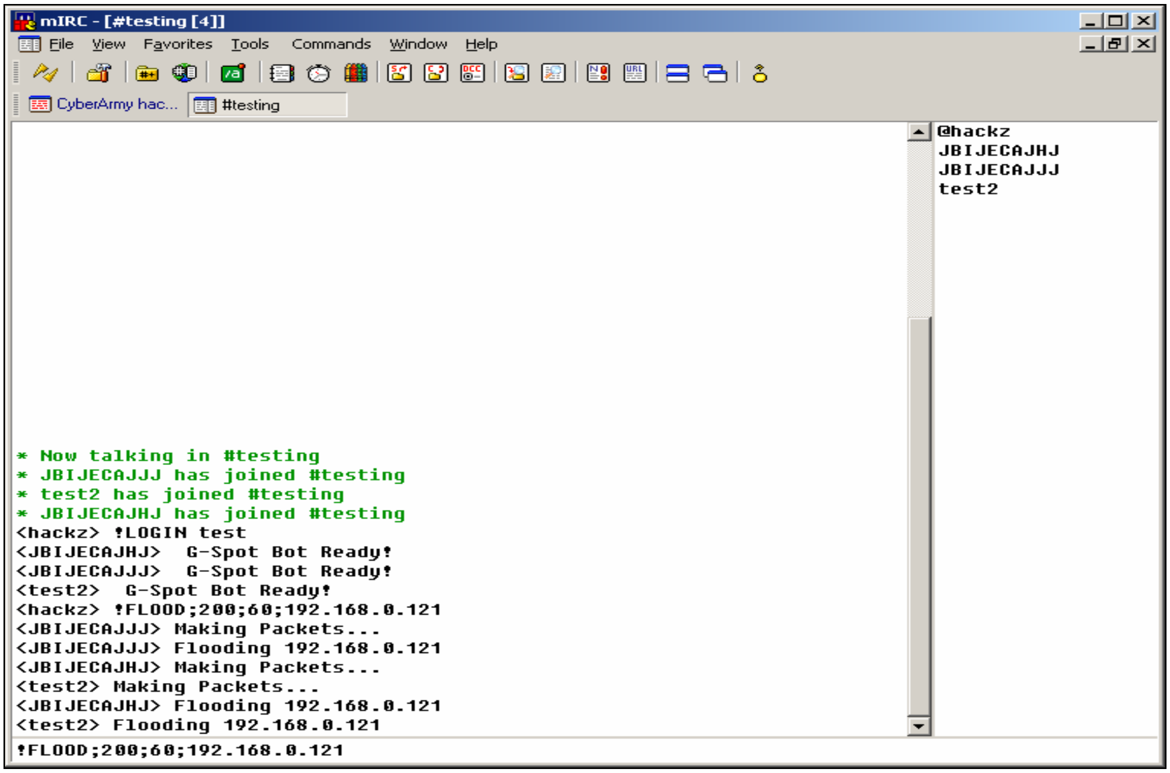
The controller has to issue an login command in the IRC channel to get control over the bots. ---!LOGIN <password>



```
* Now talking in #testing
* JBIJECAJJJ has joined #testing
* test2 has joined #testing
* JBIJECAJHJ has joined #testing
<hackz> !LOGIN test
<JBIJECAJHJ>  G-Spot Bot Ready!
<JBIJECAJJJ>  G-Spot Bot Ready!
<test2>  G-Spot Bot Ready!
```

```
@hackz
JBIJECAJHJ
JBIJECAJJJ
test2
```

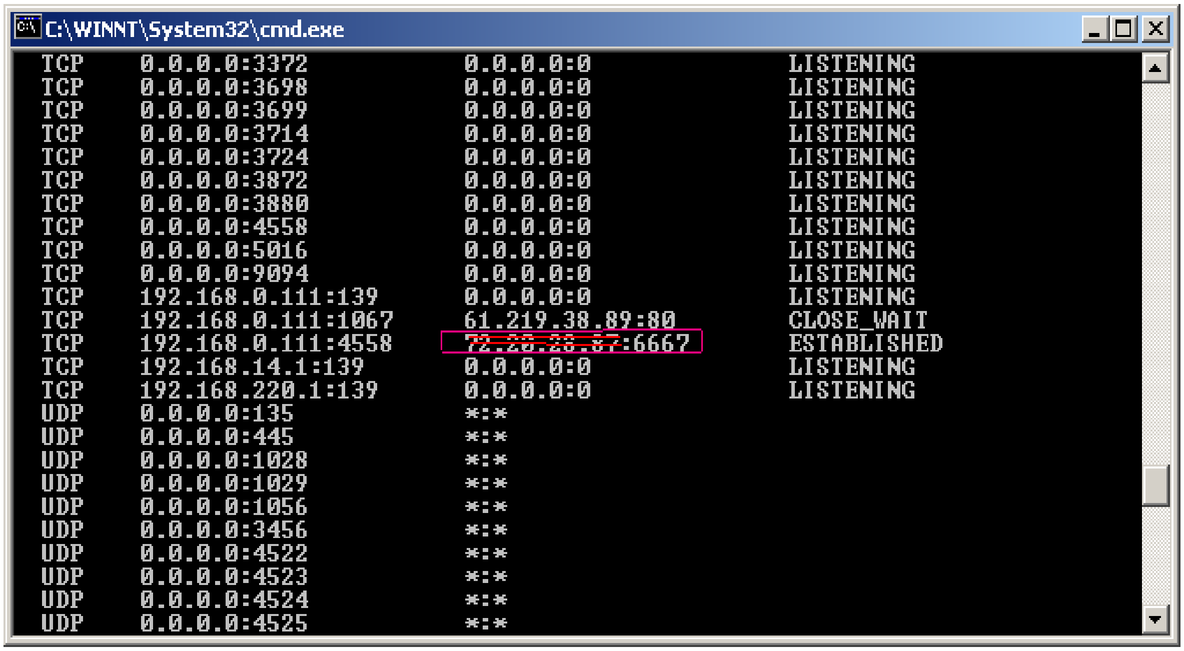
Now the bot army is ready to listen commands given by the bot controller (hackz). This particular bot is customized to launch ICMP DDoS attack.



```
* Now talking in #testing
* JBIJECAJJJ has joined #testing
* test2 has joined #testing
* JBIJECAJHJ has joined #testing
<hackz> !LOGIN test
<JBIJECAJHJ>  G-Spot Bot Ready!
<JBIJECAJJJ>  G-Spot Bot Ready!
<test2>  G-Spot Bot Ready!
<hackz> !FLOOD;200;60;192.168.0.121
<JBIJECAJJJ> Making Packets...
<JBIJECAJJJ> Flooding 192.168.0.121
<JBIJECAJHJ> Making Packets...
<test2> Making Packets...
<JBIJECAJHJ> Flooding 192.168.0.121
<test2> Flooding 192.168.0.121
```

```
!FLOOD;200;60;192.168.0.121
```

Though this particular bot does not have any visual impact on the local machine, its presence can be observed in the following way. The **`netstat`** result of the infected machine shows that the machine is connected to port 6667 of a remote machine. If the local user is not using any IRC client then such connection attempt is suspicious and indicates a possibility of bot infection. Though the TCP 6667 is the RFC defined port for IRC communication and is used most commonly, the port number may very as per the implementation of the IRC server in use



```
  TCP    0.0.0.0:3372           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3698           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3699           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3714           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3724           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3872           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3880           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:4558           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5016           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9094           0.0.0.0:0              LISTENING
  TCP    192.168.0.111:139      0.0.0.0:0              LISTENING
  TCP    192.168.0.111:1067     61.219.38.89:80        CLOSE_WAIT
  TCP    192.168.0.111:4558     ~~72.20.28.87~~:6667      ESTABLISHED
  TCP    192.168.14.1:139       0.0.0.0:0              LISTENING
  TCP    192.168.220.1:139      0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1028           *:*
  UDP    0.0.0.0:1029           *:*
  UDP    0.0.0.0:1056           *:*
  UDP    0.0.0.0:3456           *:*
  UDP    0.0.0.0:4522           *:*
  UDP    0.0.0.0:4523           *:*
  UDP    0.0.0.0:4524           *:*
  UDP    0.0.0.0:4525           *:*
```

The process list also indicates the presence of the bot -

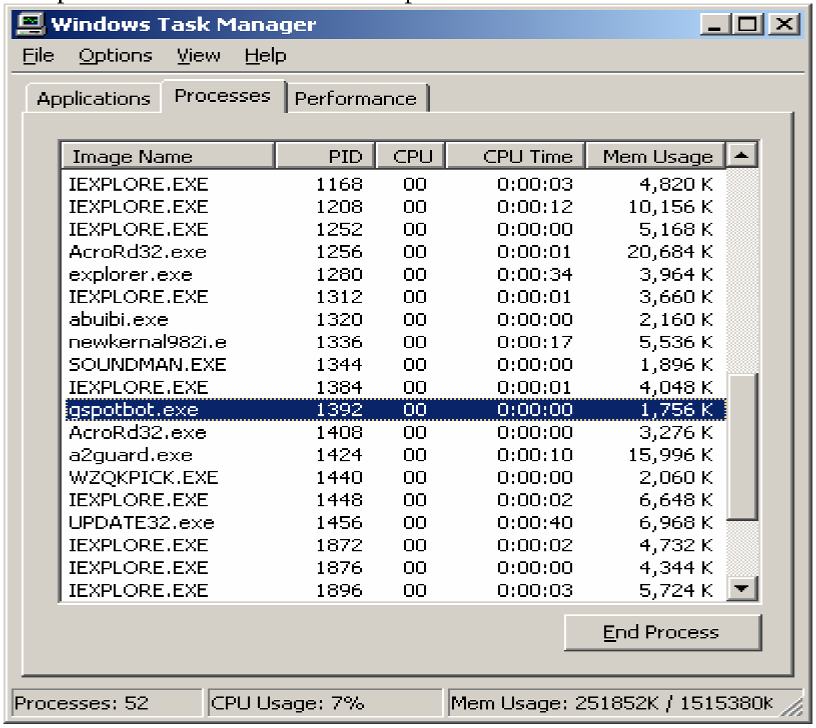


Image Name	PID	CPU	CPU Time	Mem Usage
IEXPLORE.EXE	1168	00	0:00:03	4,820 K
IEXPLORE.EXE	1208	00	0:00:12	10,156 K
IEXPLORE.EXE	1252	00	0:00:00	5,168 K
AcroRd32.exe	1256	00	0:00:01	20,684 K
explorer.exe	1280	00	0:00:34	3,964 K
IEXPLORE.EXE	1312	00	0:00:01	3,660 K
abuibi.exe	1320	00	0:00:00	2,160 K
newkernal982i.e	1336	00	0:00:17	5,536 K
SOUNDMAN.EXE	1344	00	0:00:00	1,896 K
IEXPLORE.EXE	1384	00	0:00:01	4,048 K
gspotbot.exe	1392	00	0:00:00	1,756 K
AcroRd32.exe	1408	00	0:00:00	3,276 K
a2guard.exe	1424	00	0:00:10	15,996 K
WZQKPICK.EXE	1440	00	0:00:00	2,060 K
IEXPLORE.EXE	1448	00	0:00:02	6,648 K
UPDATE32.exe	1456	00	0:00:40	6,968 K
IEXPLORE.EXE	1872	00	0:00:02	4,732 K
IEXPLORE.EXE	1876	00	0:00:00	4,344 K
IEXPLORE.EXE	1896	00	0:00:03	5,724 K

Processes: 52 CPU Usage: 7% Mem Usage: 251852K / 1515380K

Annexure II- Desktop defense reference

Microsoft Security Updates
http://www.microsoft.com/security/default.mspx

Anti Virus

AVG (http://www.grisoft.com/doc/1)
Trend Micro (http://housecall.trendmicro.com/)
Panda Soft (http://www.pandasoftware.com/products/activescan/com/activescan_principal.htm)
Trend Micro (http://www.trendmicro.com)
McAfee (http://www.nai.com)
Sophos (http://www.sophos.com)
Symantec (http://www.symantec.com/index.htm)
Computer Associates (http://www3.ca.com)

Anti Spyware
Microsoft Anti Spyware (http://www.microsoft.com/athome/security/spyware/default.mspx)
Spyware Doctor (http://www.pctools.com/spyware-doctor/)

Personal firewall
Zonal Alarm (http://www.zonelabs.com)
Sygate (http://soho.sygate.com/products/spf_standard.htm)
Kaspersky (http://www.kaspersky.com/antihacker)

Other monitoring tools
System mechanic (http://www.iolo.com/sm/index.cfm)
Registry mechanic (http://www.pctools.com/registry-mechanic/)