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

Masaru AKAI

BB Technology / SBB-SIRT

BB Technology

SoftBank

BB Technology
SoftBank

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

BB Technology
SoftBank

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.**

BB Technology
SoftBank

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.

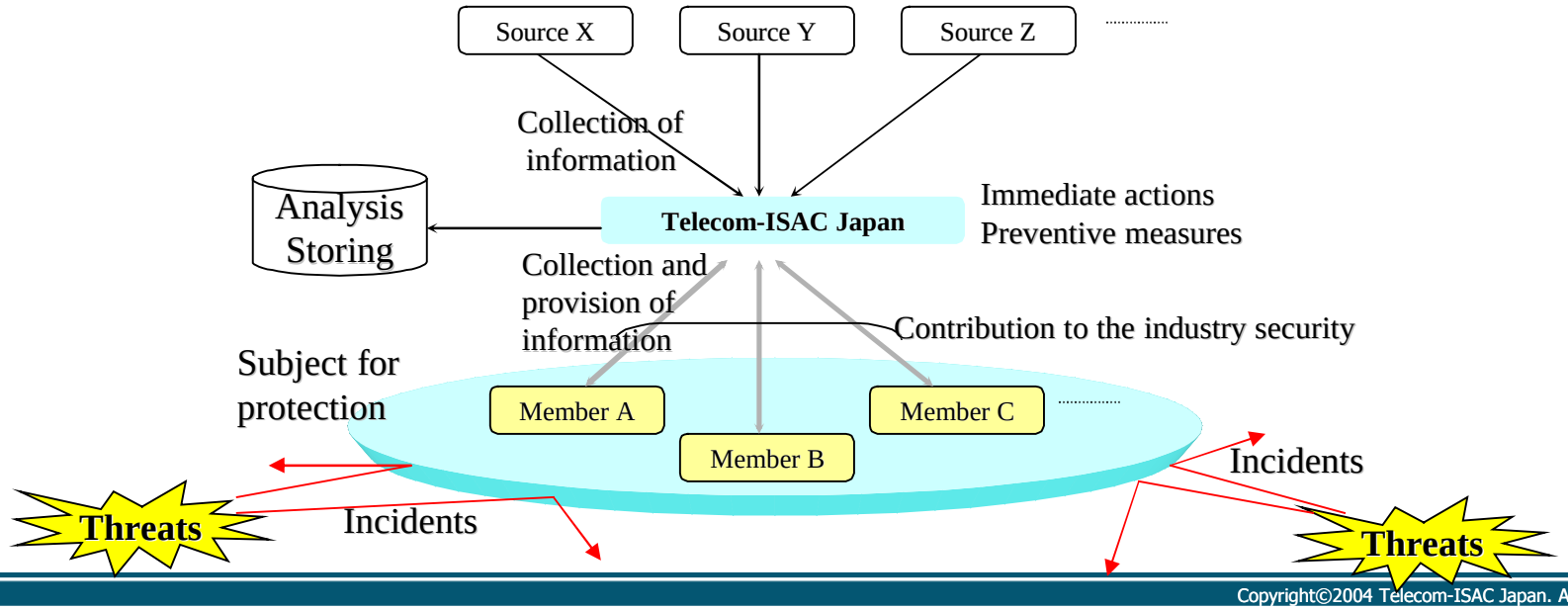
What is Telecom-ISAC-Japan ?

Telecom-ISAC Japan

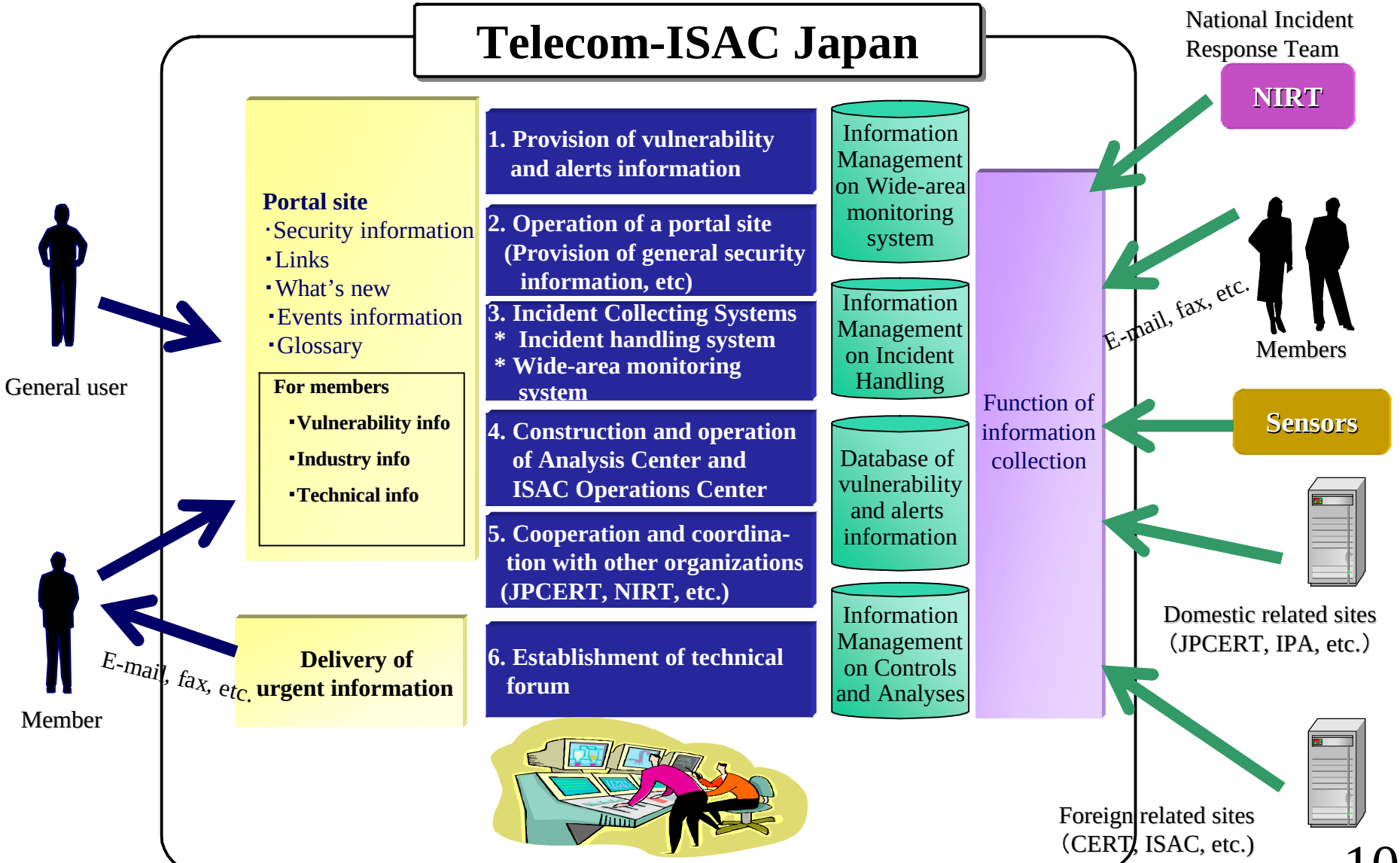
*Telecom-ISAC Japan must be managed as an independent and reliable organization.

*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

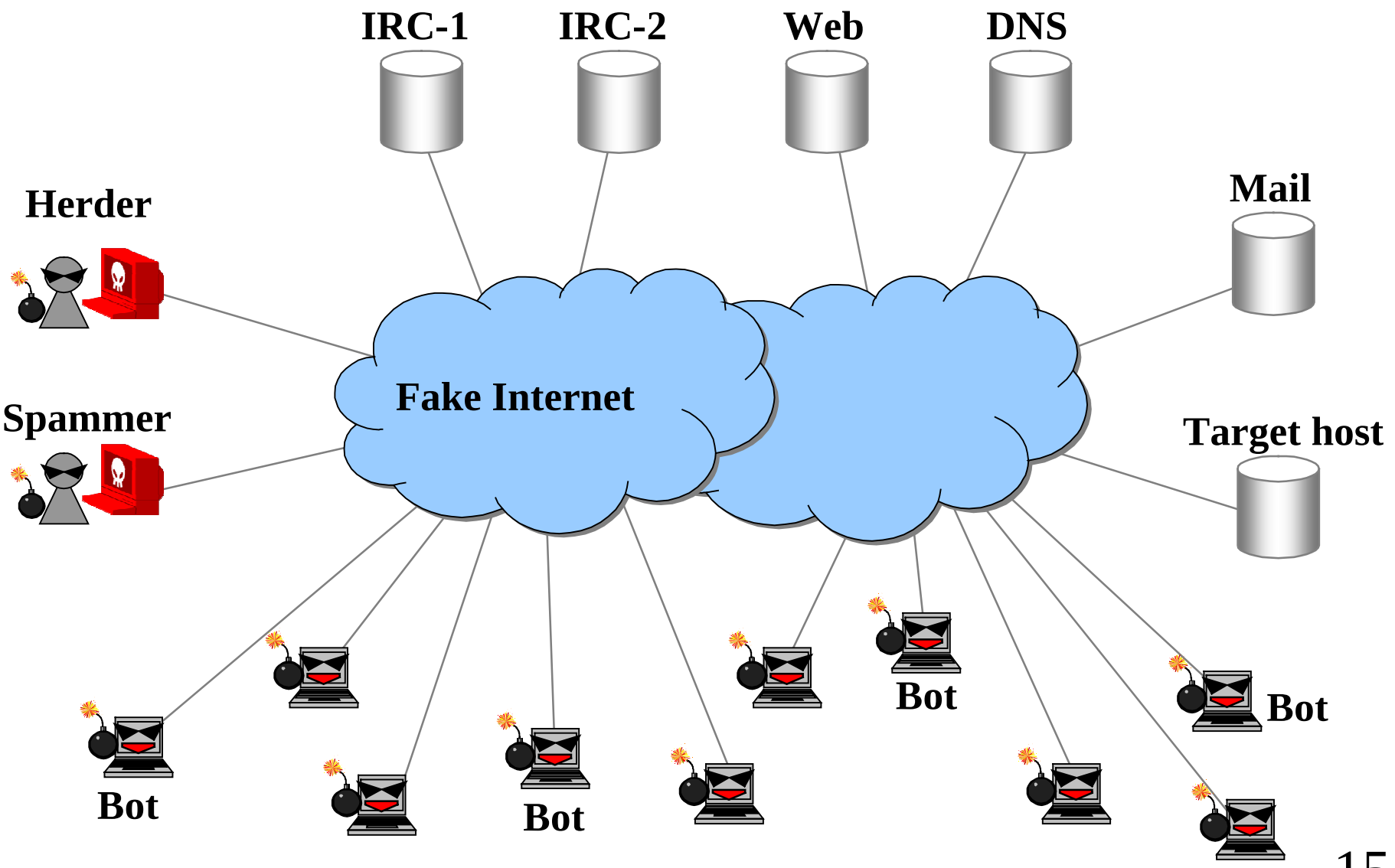
- The majority of subspecies of Bot cannot be detected even with the latest pattern file.
- One person in 40–50 Internet users is infected with Bot.
- When unmeasured PC connect to the net, it is infected in 4 minutes.
- The bandwidth being occupied by Bot is several Gbps in Japan.

Breeding record of Botnet

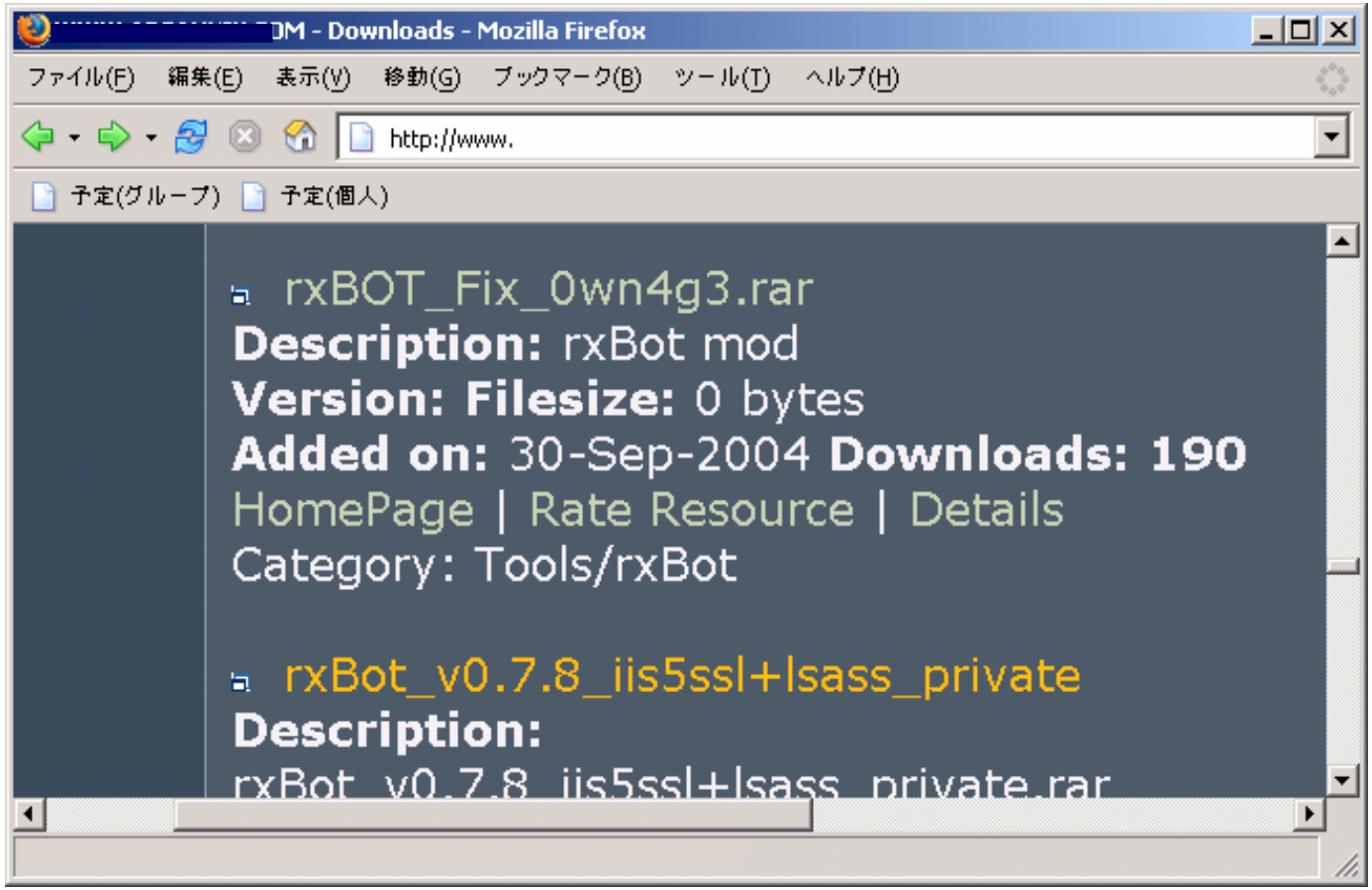
- Wild Bot is obtained.
  - Change to livestock to MyBot (Construction of Botnet for investigation environment)
- The art was trained.(Ability measurement examination)
  - Check Action, Power and Ability
- Is there a method of exterminating Botnet?

Operation
My Botnet Building

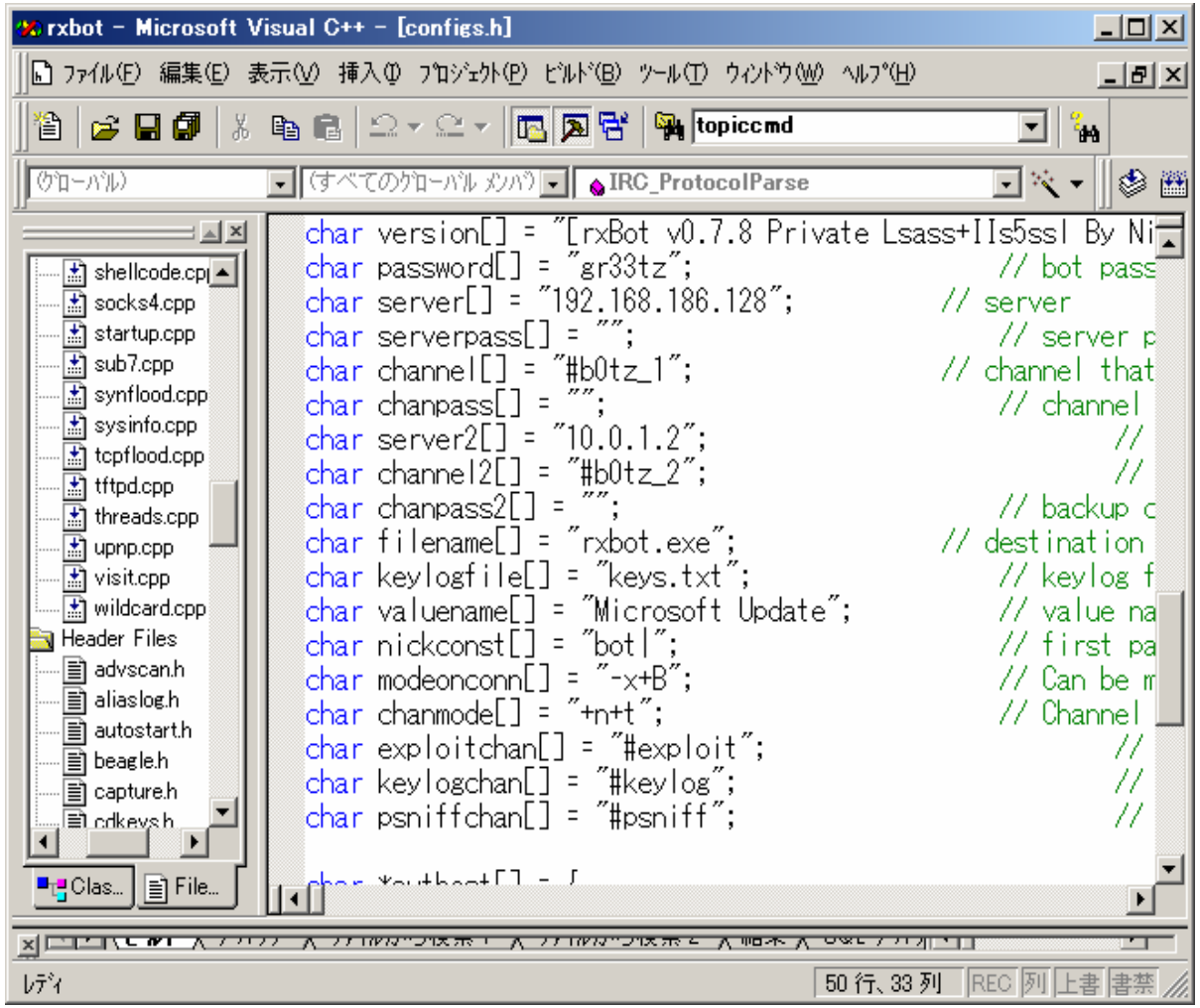
Environment for constructed Botnet investigation



Download Source code of Bot



Parameters of bot source code

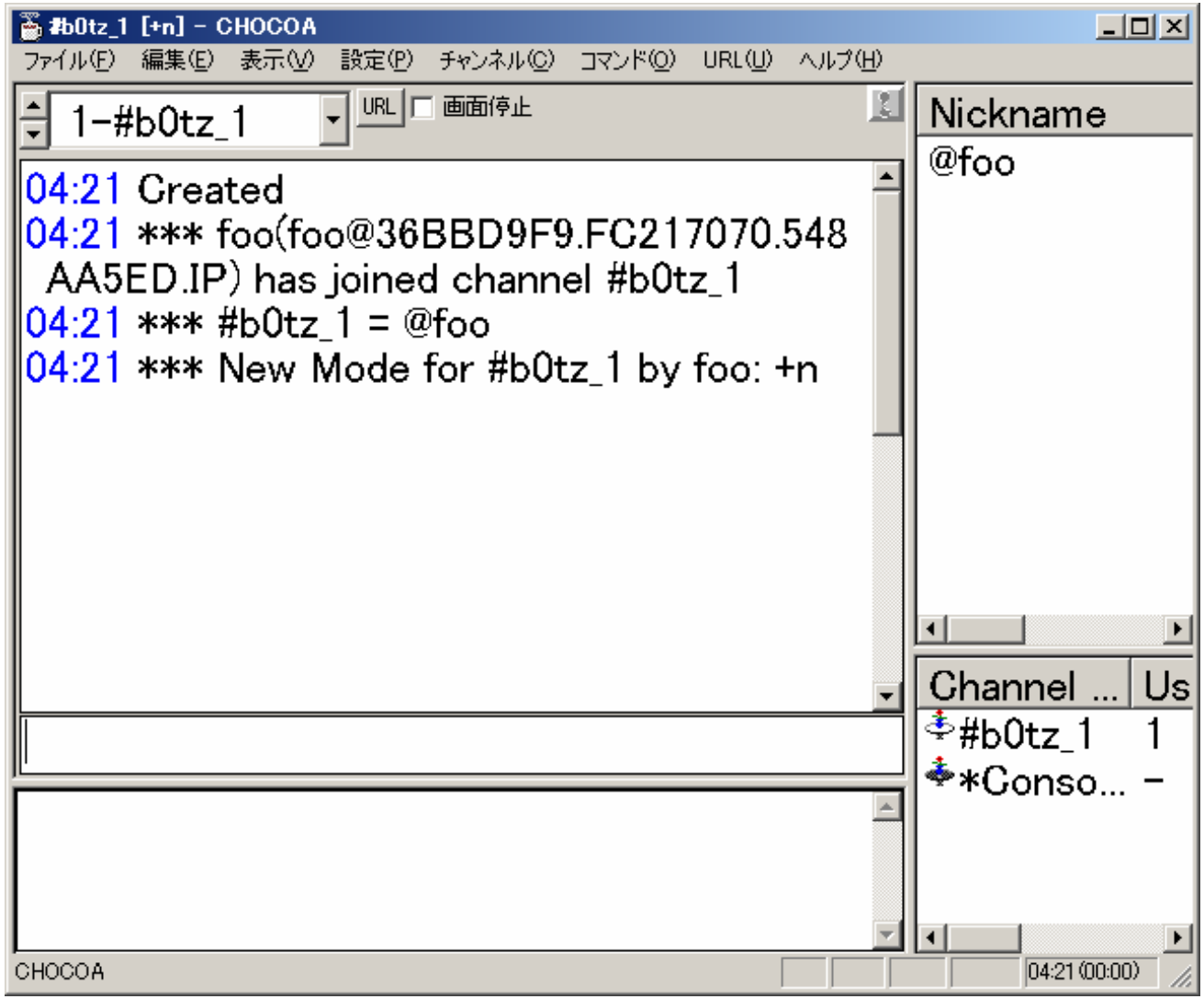


Set item concerning IRC Server

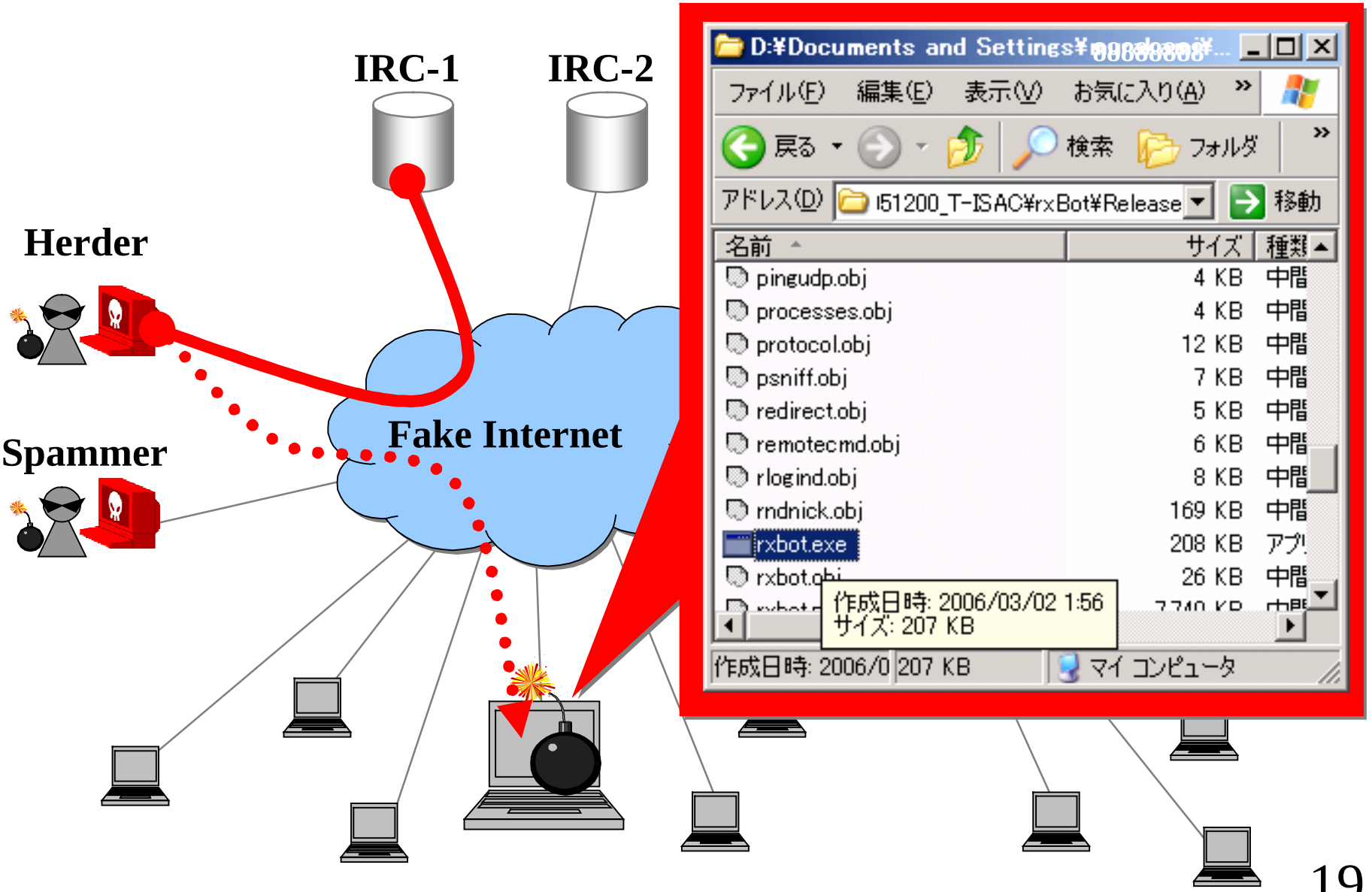
- IRC Server's IPAddress, Service port
- Backup IRC Server's IPAddress, Service port
- Herder's Auth Password
- IRC Server connection password
- IRC Channel Name, JOIN Password
- Setting concerning operation of bot
- Check of TOPICCMD etc.

Connect IRC Server as HERDER

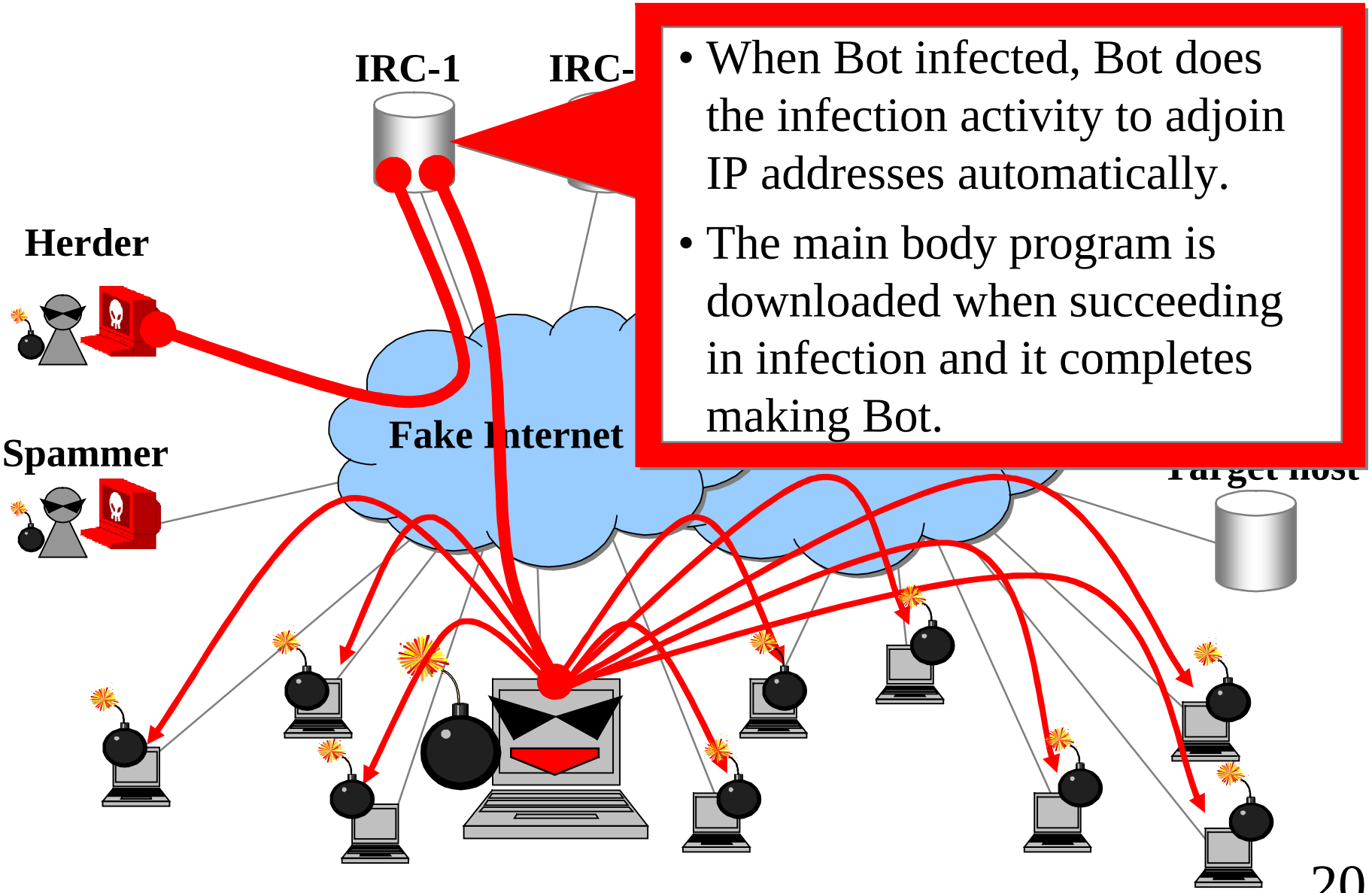
HERDER's name is "foo"



Bury bot and execution

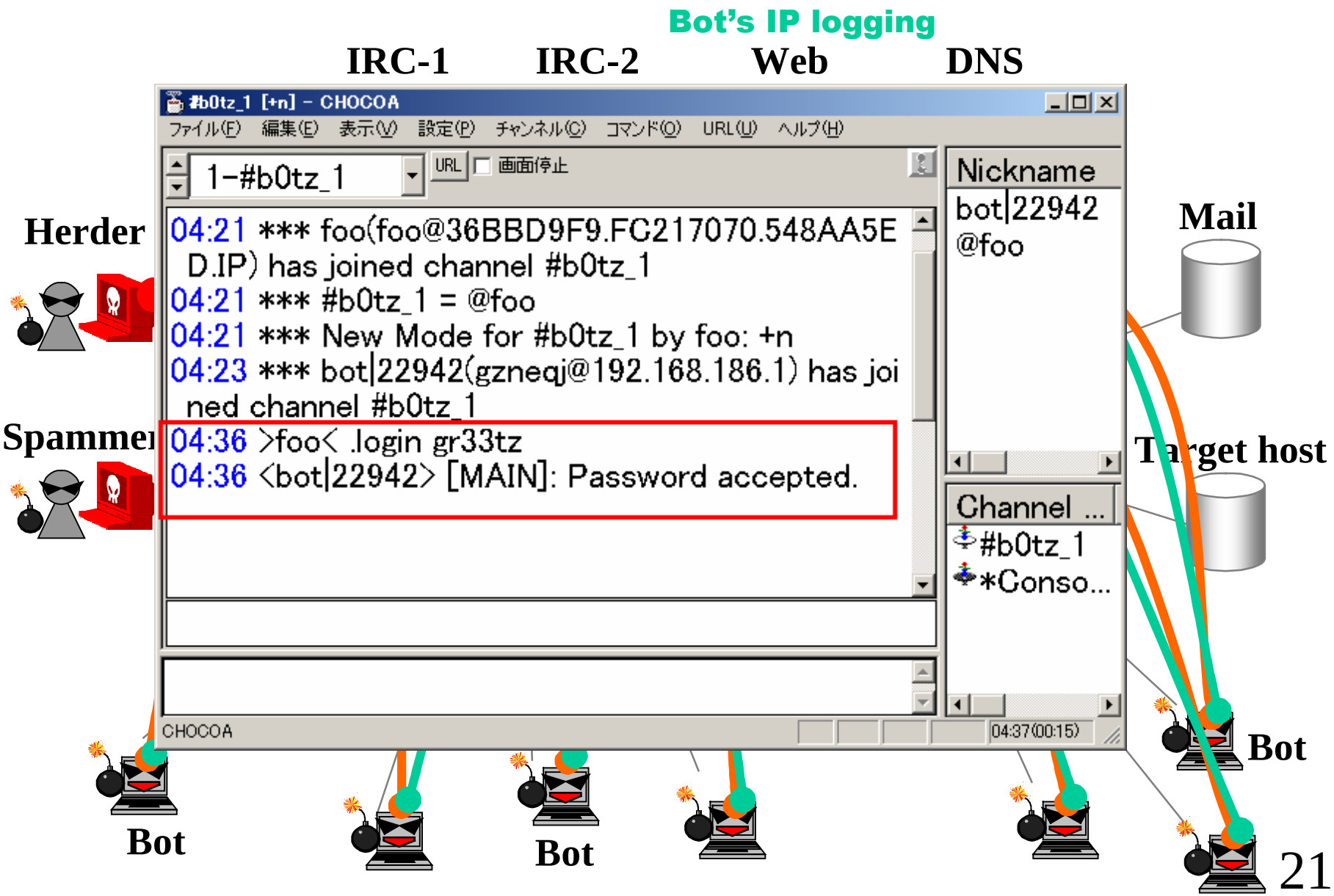


Bot expands infection, Botnet is constructed.

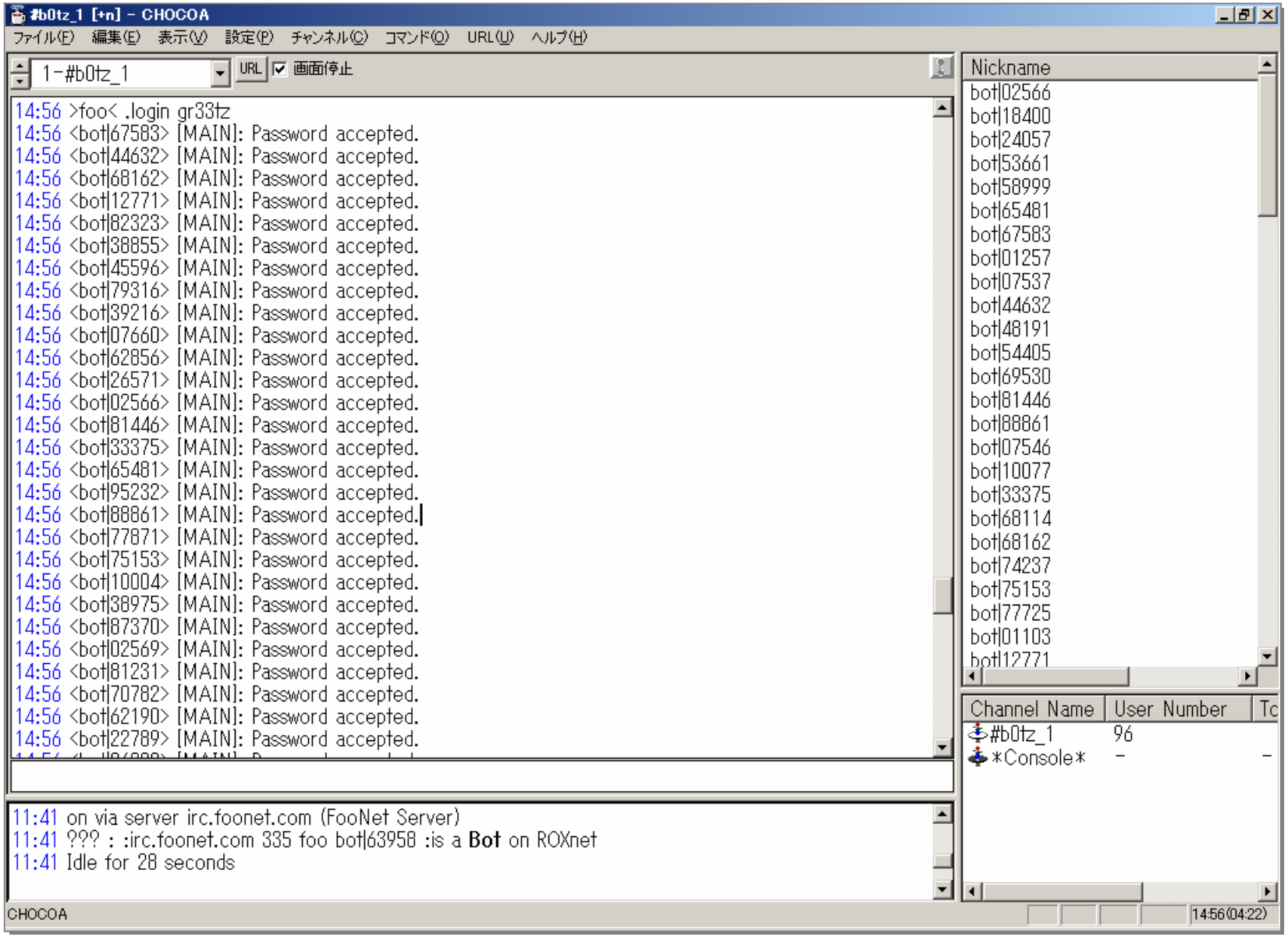


- When Bot infected, Bot does the infection activity to adjoin IP addresses automatically.
- The main body program is downloaded when succeeding in infection and it completes making Bot.

Complete to build “My Botnet”



Complete to build my Botnet

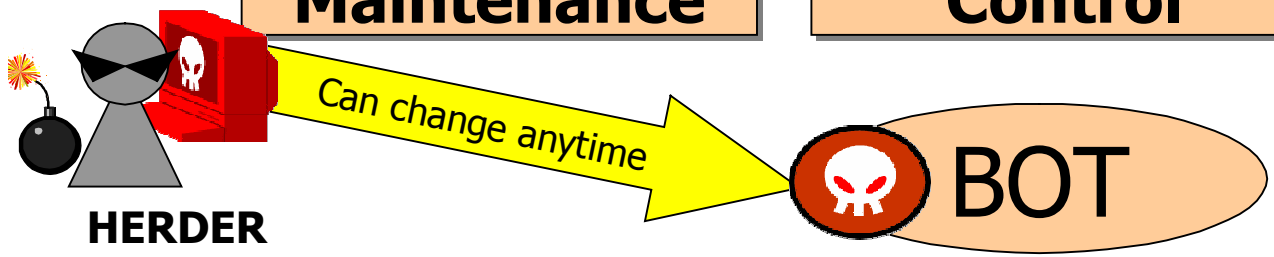


My Botnet Ability investigation

Investigation result of Source code（Agobot）

Telecom SAC Japan

Circulation of source	Auth/Encryption	polymorphic
BOT Generator	IRC	Anti AntiVirus
Version up	Original channel	Anti Debugger/VM
Maintenance	**Control**	**Self defense**



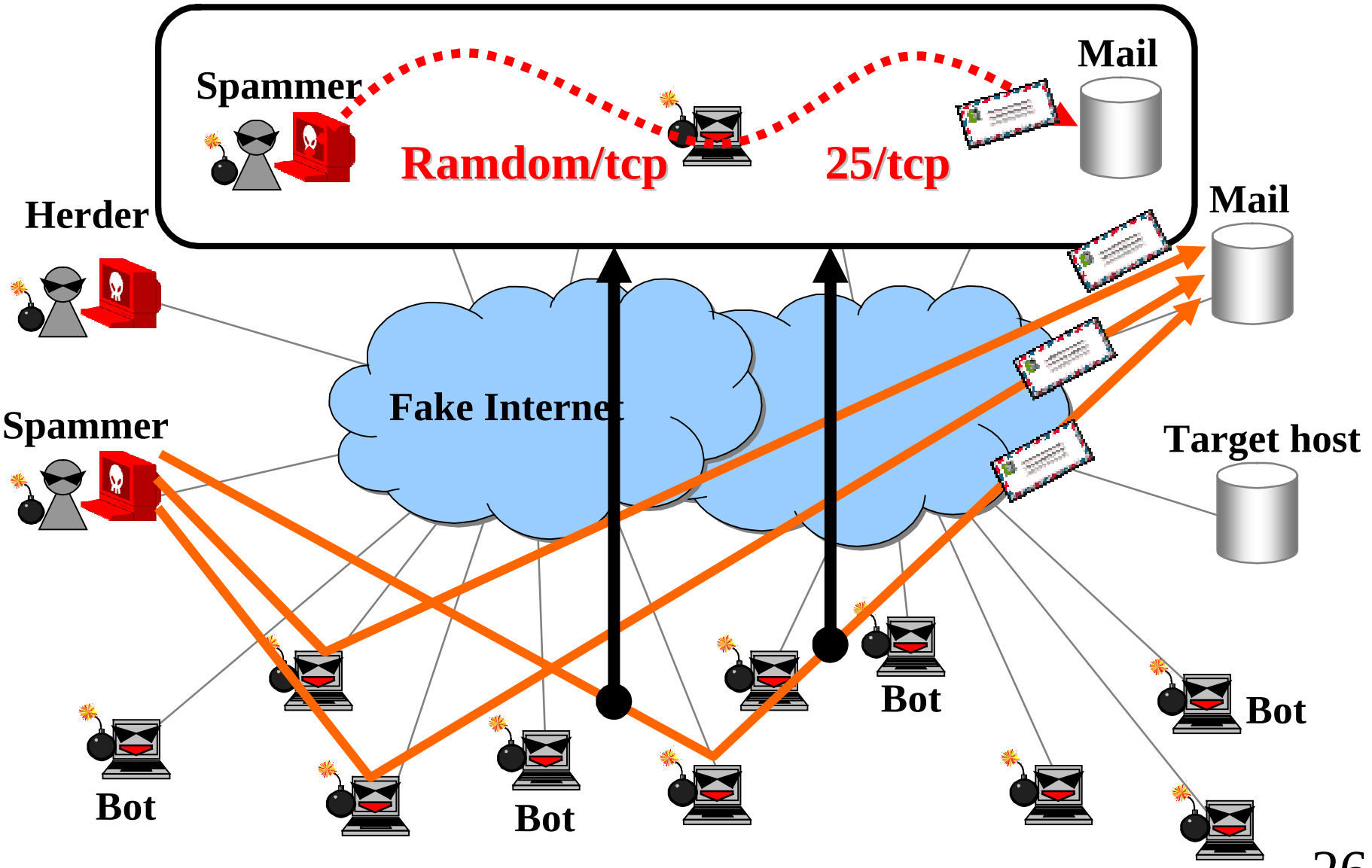
Windows

Linux

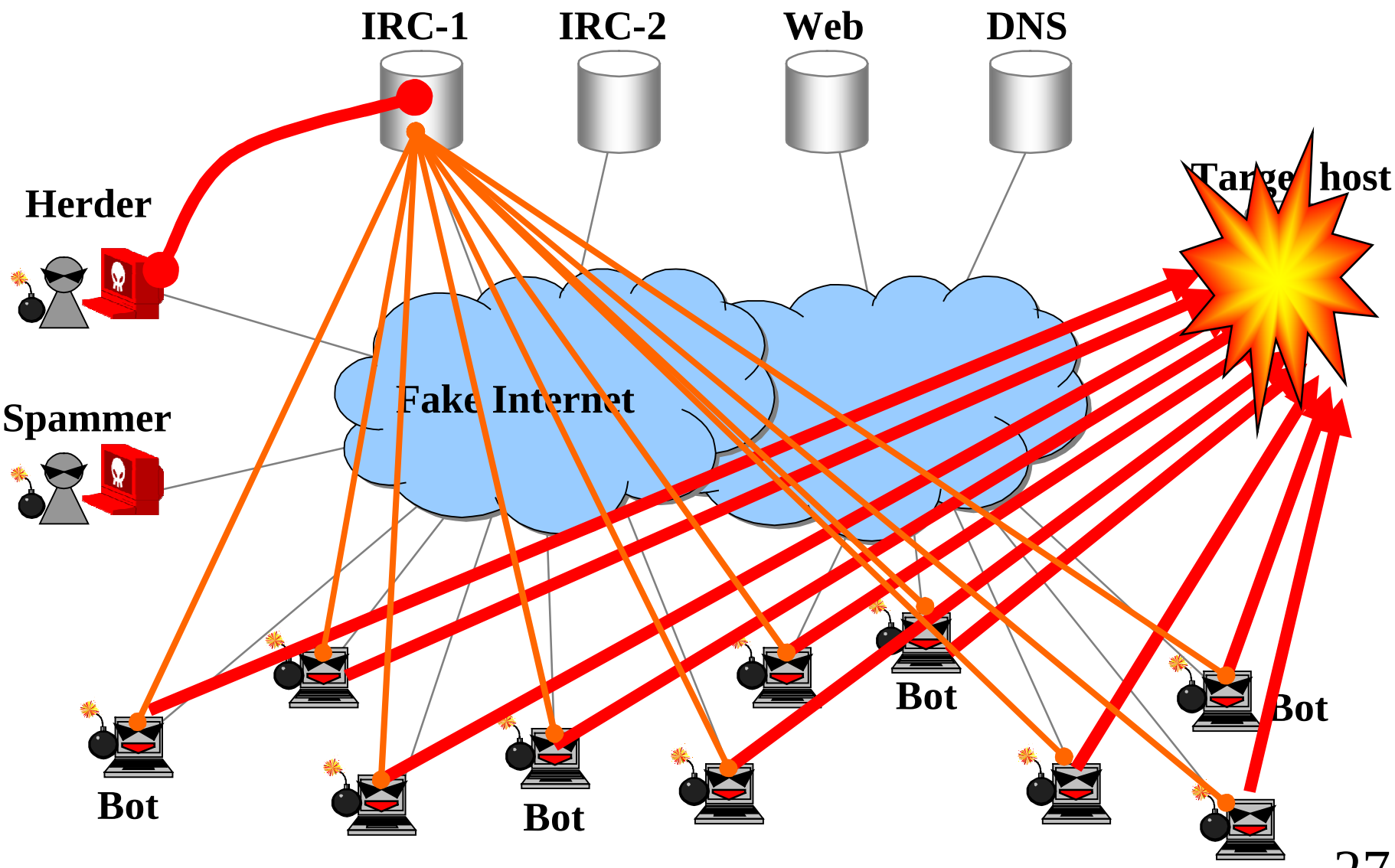
Information gathering	**Infection activity**	**Attack**
Account FTP, IRC, PAYPAL、AOL	Using vulnerability	DDoS
connection with vulnerable Clients	Using Network sharing	Exploited PCs
E-Mail, Product Key	Using Virus	SPAM Relay

Investigation of Attack function (Ability)

SPAM Mail Sending

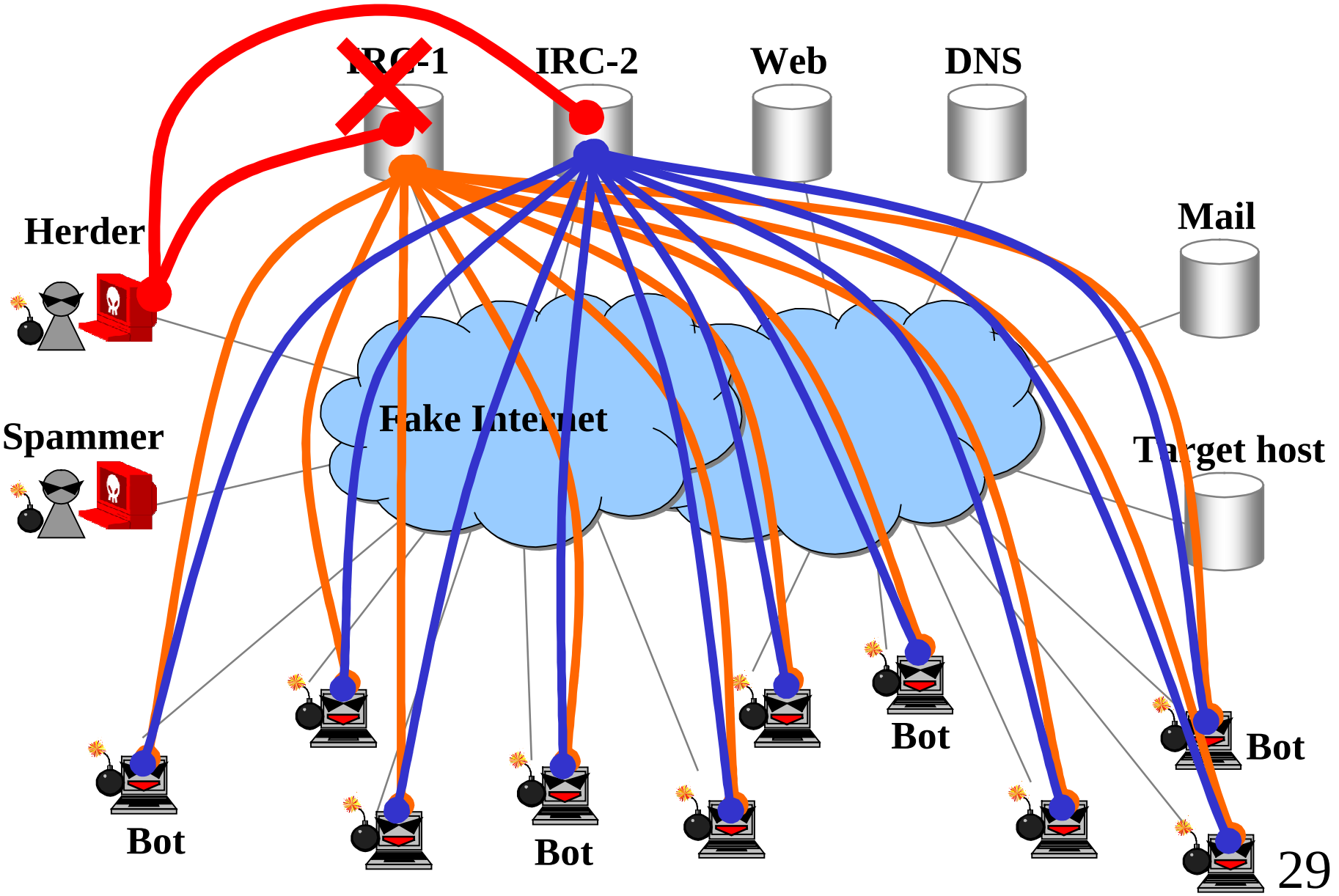


DDoS Attack

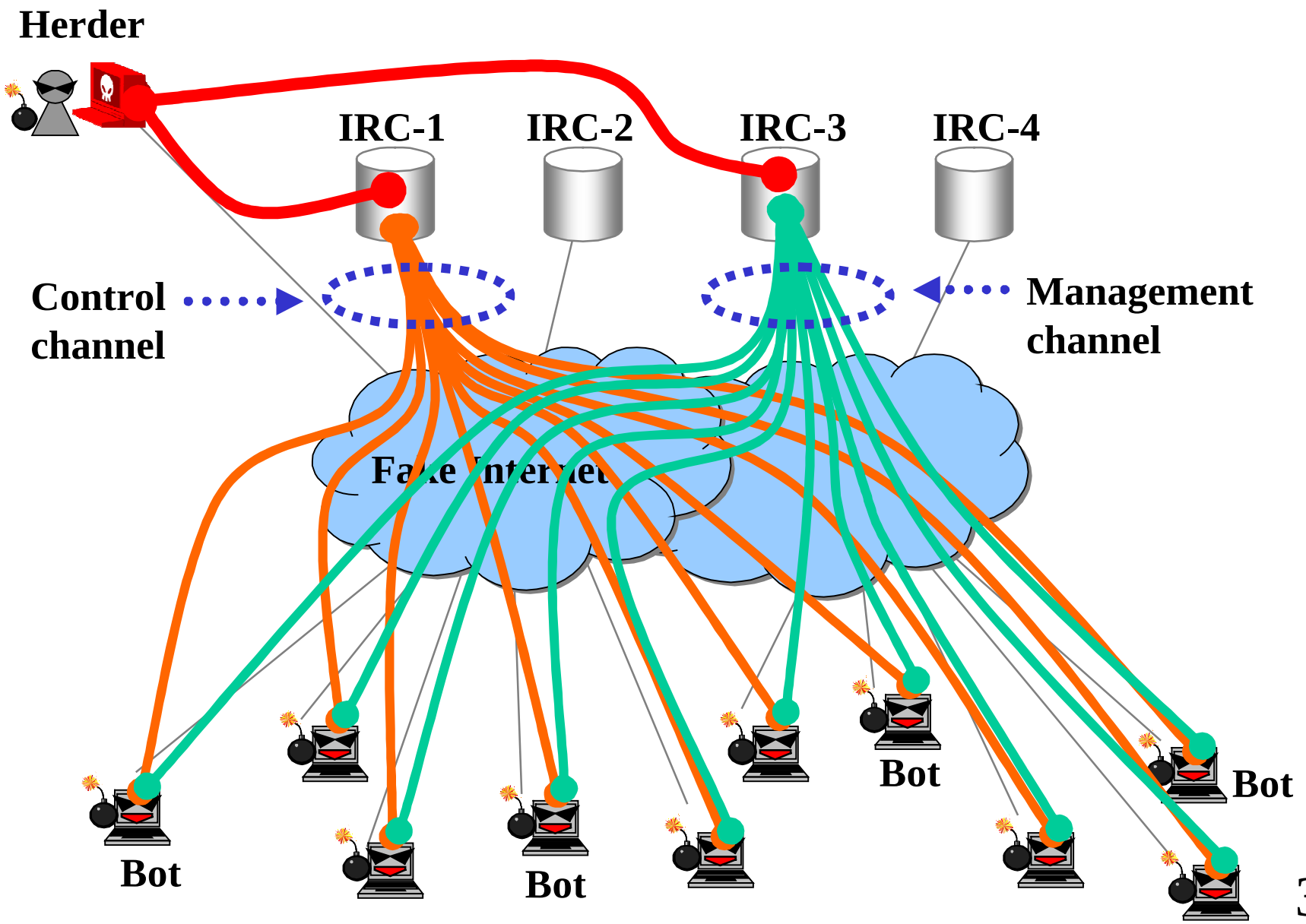


Investigation of Botnet operation

Recovery of My Botnet Completed



Form of use of IRC server



Conclusion

- 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

BB Technology
SoftBank

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.