FY 2006

Cyber Clean Center Activity Report

Cyber Clean Center

https://www.ccc.go.jp/

The Cyber Clean Center is a shared initiative of the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry.

Contents

1 Introduction

BOTs are a kind of malicious program with numerous subspecies that have recently become widespread in the Internet world. The disinfection of BOTs using conventional methods, however, has become increasingly difficult. In addition, there is a trend where the attacks and infection activities of BOTs are taken in constrained portions of programs and using stealthing techniques. Thus the stealthy nature of BOTs typically leaves users unaware of their activities. It is said that computers infected in this way form the infrastructure of such cyber attacks as spam mail, phishing, or DDoS (Distributed Denial of Service) attacks. This is a critical issue impeding the goal of a safer Internet environment.
Responding to this threat, the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry established the Cyber Clean Center (referred to as CCC hereinafter) in December 2006 to launch the “BOT countermeasure project” in which both ministries work cooperatively. Part of the CCC project is a portal site designed to effectively and safely improve understanding about BOT attacks and infection activities, identify users whose computers are attacked and infected, and provide those users with specific measures to disinfect BOTs. The underlying goal is to establish a safer Internet environment.
CCC is structured and operated as a comprehensive service for its members, such as governmental agencies, ISPs (Internet Service Providers), business entities developing BOT disinfection tools, and security vendors. This service is designed to eradicate domestic BOTs in Japan by conducting effective, continuous public awareness campaigns on BOT disinfection.

1.1 Current status of BOTs

BOTs are a kind of malicious program (malware) created to use PCs fraudulently. An attacker (also called a “herder”) with malicious intent remotely controls PCs infected with BOTs to send spam mail or cause DoS (Denial of Service) attacks on specific sites. The majority of users owning PCs infected with BOTs are thereby forced to become an intermediary for crimes and therefore not only become victims but also victimizers, although not realizing what is really happening on their PCs.
PCs infected with BOTs are automatically connected to command servers prepared by attackers to create massive networks called “BOT networks” that are subsequently used for malicious purposes.
Previously, almost all viruses were created for the pleasure of hobbyist attackers. BOTs, however, are targeted to gain commercial benefits by lending out the BOT networks on a pay-by-the-hour basis or selling the private information harvested. BOTs are so clever and malignant that the users of infected PCs have difficulty in identifying BOTs since no particular symptoms appear on the surface. Detection by anti-virus products is also proving inconsistent as many BOT programs are frequently updated and released in greater volumes.
According to an investigation conducted in 2005 by Telecom-ISAC Japan, JPCERT/CC, and others, approximately 2 to 2.5% of all Internet broadband users in Japan are estimated infected with BOTs. Assuming a total number of about 20 million broadband users in Japan, 400,000 to 500,000 PCs are estimated to be infected. This large number implies that the vast majority of Internet systems in the world could be easily simultaneously at once if cyber-attacked by these BOT-infected PCs.

1.2 Overview of CCC

Many PCs infected with BOTs lack at least one recommended security measure, such as the absence of anti-virus software or not enabling automatic Windows Update. Moreover, the users of BOT-infected PCs usually do not know that their PCs are infected, due to the stealthy nature of BOTs. CCC runs a program to notify such users about the "facts of being infected" through ISPs and urges them to disinfect BOTs.
More specifically, the process is as follows:
(1) Detecting attack events (i.e., infection activities) on BOT-infected PCs using "decoy PCs (HoneyPots)" to collect samples of BOT malware (i.e., specific programs to be analyzed);
(2) Analyzing the samples of BOT malware to create a "disinfection tool," while;
(3) Identifying the attacking source in cooperation with ISPs and sending mail to users advising them of appropriate disinfection steps, and finally;
(4) Having the users disinfect the BOT upon receiving alert mail downloaded via the disinfection tool from the BOT measure page on the CCC website.

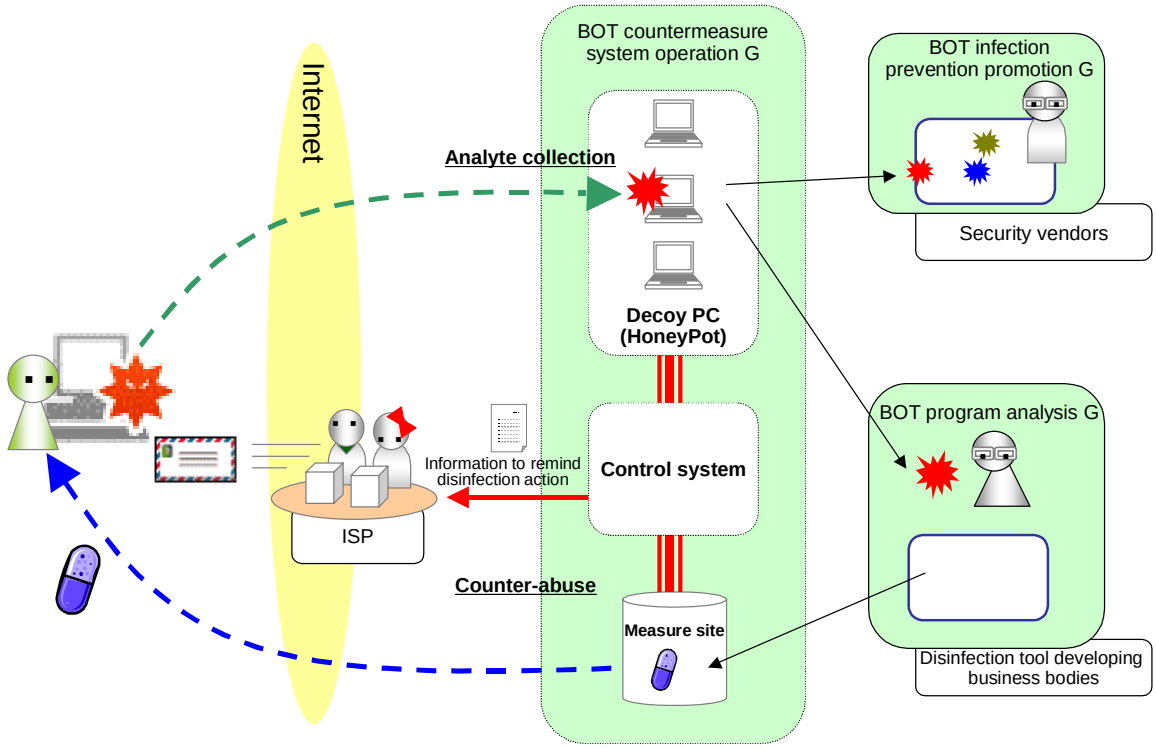

Fig. 1.2.1 CCC process for recommending disinfection action

CCC is structured and operated by the Cyber Clean Center Steering Committee (CCC-SC), along with the following three groups, depending on the nature of the work involved.

[BOT countermeasure system operation group] (Telecom-ISAC Japan)
This group operates the backbone system of this project including HoneyPots and alerts users about disinfecting BOTs through ISPs. This group also investigates the latest trends of malware including BOTs.

<Project-participating ISPs>
BIGLOBE, DION, hi-ho, IIJ, @nifty, OCN, ODN, Yahoo! BB

[BOT program analysis group] (JPCERT Coordination Center)
This group analyzes the collected samples of BOT malware (i.e., specific programs to be analyzed for their features and techniques used). This group also conducts studies on effective analysis systems and develops countermeasure techniques in cooperation with disinfection tool developers.

<Disinfection tool developer>
Trend Micro Incorporated

[BOT infection prevention promotion group] (Information-technology Promotion Agency, Japan)
This group promotes the prevention of BOT infection by administrating the overall BOT malware samples collected by CCC and providing the samples to individual project participating security vendors for incorporation into the pattern files of the vendors' anti-virus software.

< Project participating security vendors>
Microsoft Corporation, Sourcenext Corporation, Trend Micro Incorporated, McAfee Incorporated and Symantec Corporation

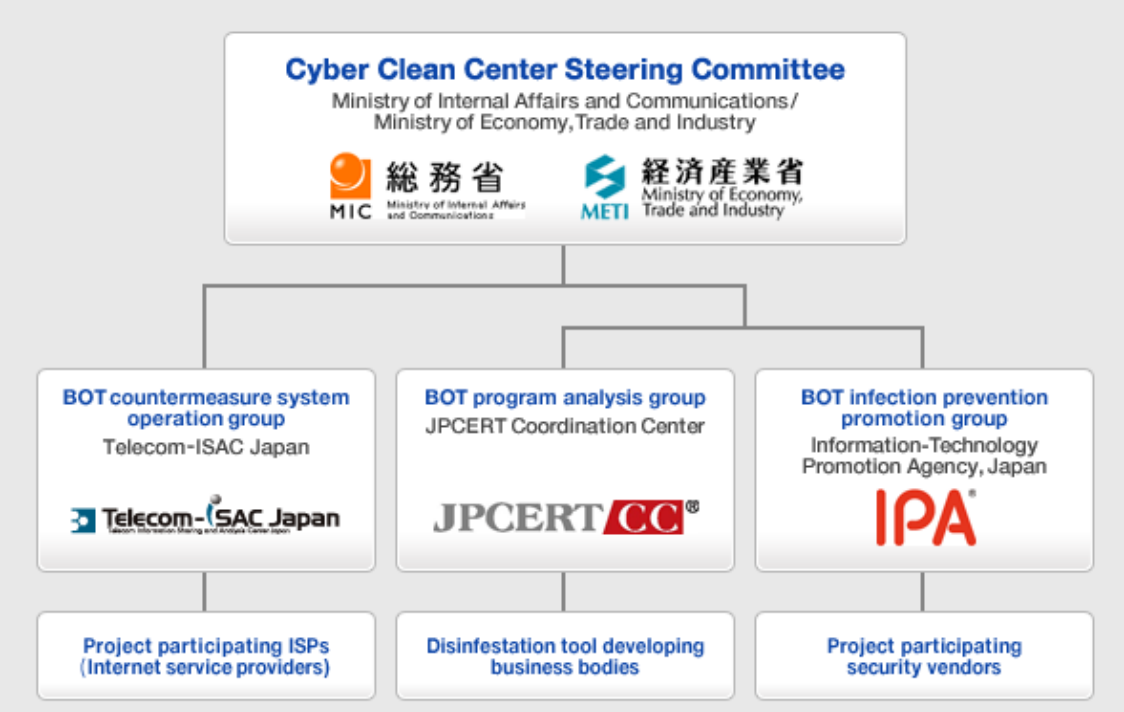

Fig. 1.2.2 CCC operation structure

2 Activity report - BOT countermeasure system operation group

2.1 Overview

The BOT countermeasure system operation group detects attacking events (infection activities) from PCs infected with BOTs, then collects and transfers BOT analytes to the BOT program analysis group.
In addition, this group identifies infected PCs to alert the users of such PCs, and appropriately manages BOT disinfection tools prepared by the BOT program analysis group for distribution to those users.

Typically, delivering uniform mail is considered the most effective way of alerting the users of PCs infected with BOTs. However, since most users are not considered knowledgeable about security measures, taking specific measures based on such uniform notification may be difficult for them. Thus, this group has adopted in cooperation with ISPs a so-called custom-made treatment, whereby infected PCs are identified, attention is raised regarding the fact of infection, and users are urged to take disinfection action.

To conduct this custom-made treatment, the infected PCs must be correctly identified. Therefore, the detection of infection activities on infected PCs is essential. For this purpose, this group deploys a number of decoy PCs so that infection activities are safely and precisely detected, the types of BOTs analyzed, and the infected PCs identified.

2.2 Analyte collection/attacking event detection

2.2.1 Overview of analyte collection

Before alerting the users of BOT-infected PCs, attacks (i.e., infection activities) from the BOT-infected PCs should be detected to collect BOT analytes. There are several known types of BOT infection activities, such as the worm type, mail attachment type, P2P type, and Web type. This project focuses on the worm type that targets the weaknesses of PCs. Consequently, decoy PCs (honeypots) intentionally left with weaknesses are deployed for detecting infection activities.
Honeypots used in this project effectively cover broad ranges of IP addresses issued by ISPs participating in this project in order to collect BOTs active in address ranges adjacent to the original addresses.
Various aspects of honeypots used for collecting BOT analytes have been studied worldwide. In this project, the primary purpose of collecting analytes is not only to collect various types of BOTs but also to ensure that the users of infected PCs are alerted as a trigger to take disinfection actions. In this way, ingenious techniques are employed to clearly identify where and when a particular analyte is transmitted.

2.2.2 Achievements

The table below lists the data collected since the detection of BOT attacking events began on November 24, 2006, until the end of March 2007. The data includes the detection count of attacking events (only for BOT analytes collected in complete form), the number of analytes (types categorized by hash value), and the number of analytes unable to be detected by commercially available anti-virus software among all analytes collected. Note that this study was transferred to and has been utilized in full-scale operation since February 6, 2007, although in the initial stages of this project, the study focused on temporary operation in a small-scale verification system.

Table 2.2.1 Detection count of attacks and number of analytes

Detection count of attacking events	974,999
No. of BOT analytes (by type)	31,082
No. of analytes unable to be detected by commercially available anti-virus software	1,711

About 500 types of BOT analytes were detected daily, among which 20 to 30 types were BOTs unable to be detected by commercially available anti-virus software.

During full-scale operation (since February 6, 2007), detailed analysis was conducted regarding the senders of BOTs detected in attacking events. The IP addresses of the senders were analyzed on a day-to-day basis for identifying the ISPs to which the addresses belong: ISPs participating in this project, other domestic ISPs, or ISPs outside Japan. The results are shown below.

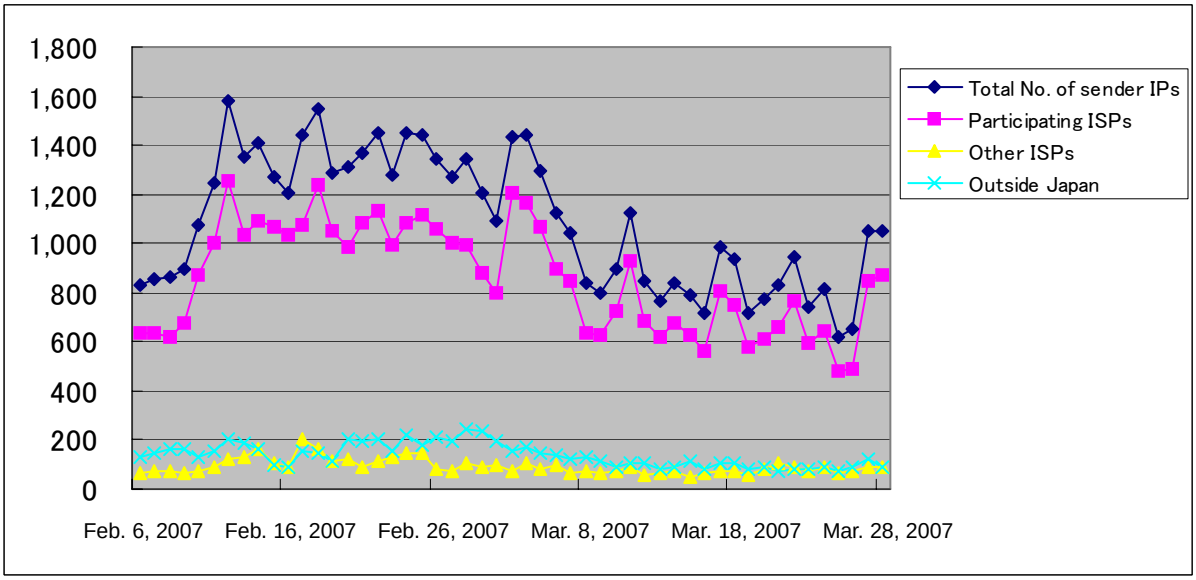

Fig. 2.2.1 Number of sender IPs in attacking events per day

The table below lists the average numbers of sender IPs in attacking events per day. About 80% of the attacks were shared by those from IPs that belong to ISPs participating in the project.

Table 2.2.2 Number of sender IPs in attacking events per day

	Participating ISPs	Other ISPs in Japan	Outside Japan
No. of sender IPs [IP/day]	858	93	137
Ratio [%]	78.9%	8.5%	12.6%

Attacks from outside Japan are counted for the top ten countries as follows: China (CN), Taiwan (TW), Korea (KR), U.S.A (US), Hong Kong (HK), Philippines (PH), India (IN), Malaysia (MY), Thailand (TH), and Vietnam (VN). The results show that attacks from Asian countries, which have IP address ranges adjacent to Japan's, share most of the attacks.

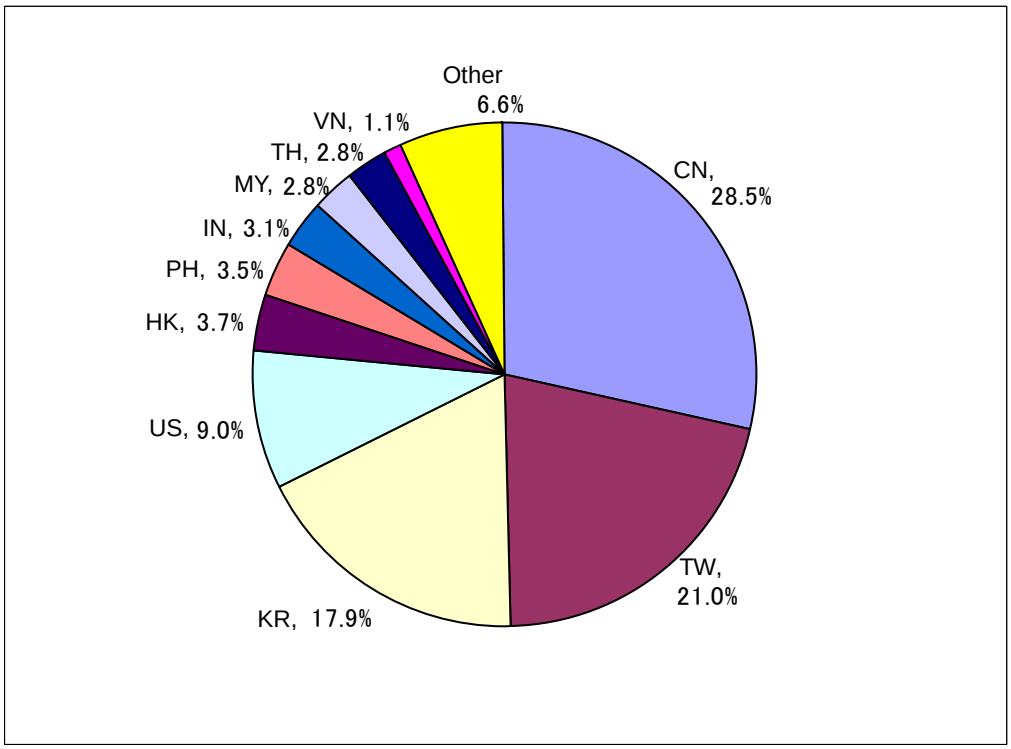

Fig. 2.2.2 Percentage of attacking events from outside Japan

This project expects that infected PCs on which analytes are detected will be those subject to alerts issued through participating ISPs. Thus, the IP addresses controlled by those ISPs are designated for assignment in honeypots. Based on the results above, BOT infection activities limited to IP addresses adjacent to the addresses for infected PCs were reconfirmed.
In order to expand cooperative work with ISPs or CATV not currently participating in this project, it is considered effective to assign IP addresses controlled by such ISPs or CATV to honeypots.
Domestic attacking sources other than participating ISPs or ISPs/CATV listed above include business entities and schools. To achieve the goal of this project, studies on these sources are also essential.

2.2.3 Future Development

2.2.3.1 Advanced Honeypots

Existing honeypots should be extended to allow for more effective alert activities. Specifically, the following should be studied: expanding the subject range of operating systems (OSs) currently adopted for honeypots toward a range closer to that of user environments, expanding the area of collecting analytes (with current access points only in Tokyo), and studying specific plans and estimating effects.

2.2.3.2 Study on new analyte collection techniques

The types of analytes subject to collection, currently limited to the worm type targeting OS weaknesses, will be expanded to include various types such as the P2P type and Web type, so that a broader range of users with infected PCs will be alerted.

2.3 Alerts

2.3.1 Abuse handling at ISPs and issues

In this project, alert action follows the procedure of analyzing the communication of BOT analytes captured by honeypots and sending mail to the senders using infected PCs in order to notify them of BOT infection and urge disinfection. This communication analysis conducted by the CCC HoneyPot operation group provides the IP addresses of senders and information about the time when the senders send out BOTs. Consequently, although information based on which ISP controls such IP addresses is provided, no contact addresses of the senders (e.g., mail addresses) can be identified.
When individuals or organizations are victimized by "inappropriate behavior through the Internet," no direct contact to the behaving party or performer is available even if the victims expect to notify the performer for correction. Moreover, there are no organizations available that can comprehensively handle such incidents. As a result, the victims must obtain the IP address of the performer and then request ISPs to handle the situation.
At each ISP, a department is established to assume the role of "abuse handling" as a primary task in order to handle the unlawful use of services or nuisances caused by its users. The term "abuse" originates from "abuse," the name of a mailbox defined in RFC 2142 (*Note) for the task of "providing a contact address when inappropriate behavior is observed in public."
* Note RFC: A series of documents disclosing studies on standards for the Internet community in IETF (Internet Engineering Task Force)

In this project, cooperative work with the abuse-handling departments at project-participating ISPs is also necessary for investigating specific approaches to take for the users of infected PCs. The technique of requesting an abuse-handling department for an alert is typical in areas such as spam mail. Still, due to the nature of such a technique, many issues are involved. In order to alert numerous users in a short time and at the lowest cost possible, it is necessary to understand the abuse-handling work performed at ISPs, overcome issues in seamless cooperation with each ISP, and establish appropriate alert processes.

2.3.1.1 Overview of abuse-handling work at ISPs

An abuse-handling department is created as one of the administration departments at many ISPs. This is because a series of work, such as identifying a user behaving as a performer to make contact, as well as stopping the provision of services and canceling membership if necessary, is considered within the scope of customer services.
However, there is a great difference between the work conducted by general customer administration and abuse handling in terms of the knowledge and experience required. More specifically, the processing of abuse handling requires the following knowledge and experience.

● Knowledge about the network
When a declaration of abuse is received, the personnel at the ISP in question must confirm that a member

of the ISP is responsible for the abusive behavior. For example, when abuse is declared with spam mail, the personnel must possess the knowledge necessary to determine whether the “From” address or mail header of the mail is not camouflaged.

● Knowledge about legal matters

Since the Telecommunications Business Law regulates ISPs operating as telecommunications companies, some pieces of useful information or techniques may not be used for investigative purposes or measures even if in the hands of service providers. Moreover, forcing a member to cancel membership for services may not be allowed, since such a measure may violate the member’s rights as a consumer even if fraudulently using the services. Therefore, a person in charge of abuse handling must possess the skills necessary to determine each case of abuse based on such knowledge regarding legal matters.

● Experience in user behavior and claims

A person in charge of abuse handling may encounter various claims reported. Such claims originate from declarers victimized by abuses and particularly by users when certain measures are taken.

Not many people possessing the necessary knowledge and experience described above are available. At many ISPs, abuse-handling operations are performed by customer service departments through a procedure based on a policy initially determined through cooperative discussion among expert departments related to abuses, and then the policy determined is forwarded to the customer service departments.

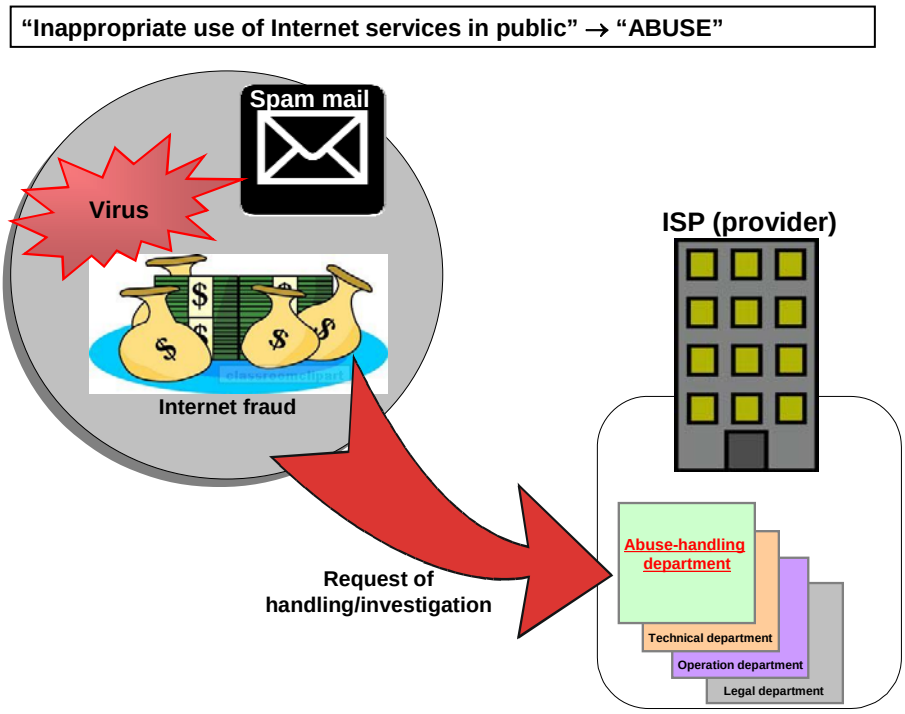

Fig. 2.3.1 How to handle abuse

2.3.1.2 Issues regarding abuse-handling practices

As mentioned above, only limited resources are available to handle abuse-handling requests or claims received from individual or organizational users. In addition, some security vendors collect information

about access by spam mail and viruses, and mechanically transfer such data attached to handling request mail to ISPs.
Abuse handling staff at the ISPs handle such requests, depending on IP addresses and time stamps in order to identify the subject user. However, since such work is very time-consuming and the personnel who can refer to information stored in the customer management system or on the authentication server are limited, such work is typically difficult and repetitive.
ISPs consider abuse-handling work part of their social responsibility. The department handling abuse remains one of the cost centers and adding resources are not easy.
Thus, mitigating the burden on abuse-handling departments at project-participating ISPs should be taken into account when establishing an alert process in cooperation with ISPs.

2.3.2 Overview of alerts

When a process to alert the users of infected PCs for BOT disinfection is established, mitigating the burden on ISPs must be taken into account, and the alerts issued must be sufficiently effective for the users of infected PCs in terms of ensured reception of alerts and implementation of BOT disinfection. This project is aimed at establishing an effective process, while requesting the opinions of experts possessing extensive knowledge in the area of customer support.

2.3.2.1 What is required for an alert process?

● Cooperation with ISPs
There exists a proposition that, while there is a lack or resources for handling abuses, alerts must be issued quickly to a broad range of users in order to have their PCs disinfected and maximize the effectiveness of alerting, based on considerations about the nature of BOTs.
In this project, specific items that increase the burden on abuse-handling work at ISPs are as follows:

(1) Work to identify clients
(2) Work to transmit alert mail
(3) Work to support users (handle requests)

These types of work require a mechanism to mitigate the burden on the ISP. Among the three items above, the work to identify clients is relegated to each ISP, since the specifications of the customer management system or authentication server differ among the ISPs. This project can mitigate the burden of the other items by providing applications and other resources for ISPs.

Abuse handling by ISPs as a part of their primary tasks is understood as being reasonable, and a reason is assumed to exist for “inappropriate behavior in public using services provided by ISPs.” When a user of an infected PC infects equipment installed by this project, it is highly likely that the infection will become widespread throughout the Internet. This understanding has been determined as adequate reasoning for requesting ISPs to handle abuses.

● Quick responsiveness
One characteristic of BOTs is that they upgrade themselves through external remote control to avoid detection by the pattern files of anti-virus software. Given this characteristic, it is simply assumed that disinfection may not be possible on a user’s PC even though disinfection is successful using a disinfection tool after the BOT is captured at a honeypot. This situation could easily occur because for a user to

actually attempt disinfection takes a certain amount of time, during which the BOT may have already been upgraded.
Therefore, in order to establish a series of processes to identify users, develop disinfection tools, and alert users, related groups must be seamlessly cooperative to maximize effectiveness.

● Wide range of users of infected PCs

An investigation revealed that the number of users of infected PCs is not concentrated on a particular ISP or network, but uniformly dispersed among multiple ISPs or networks. Handling the users of infected PCs therefore requires a structure where multiple ISPs work cooperatively in alerting those users.

2.3.2.2 Mechanism for alerting

In this project, the following work model was designed as a mechanism focused on ISPs that can continuously issue alerts as regular work, as described in the previous section.

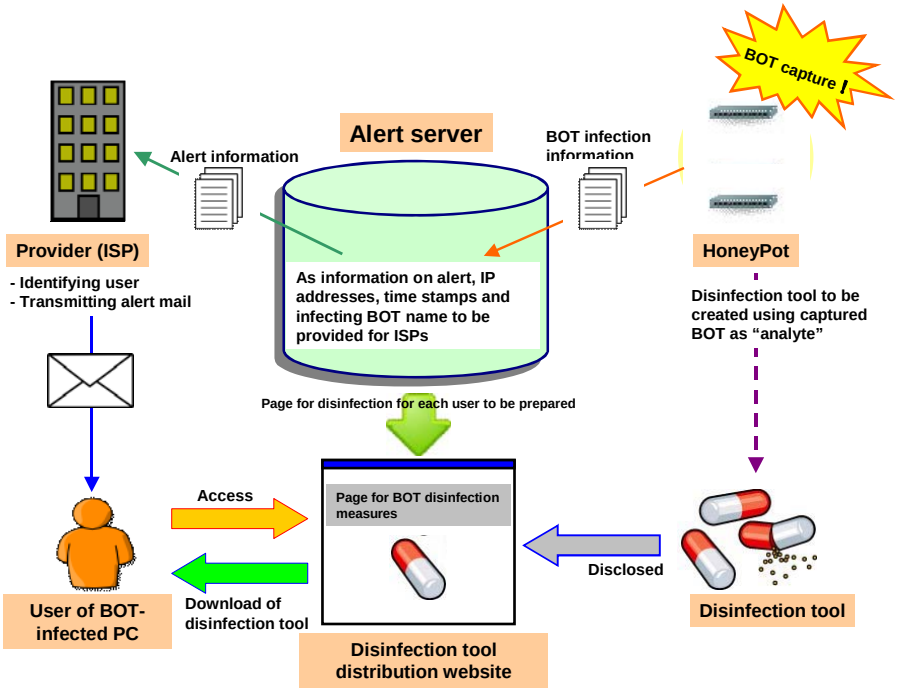

Fig. 2.3.2 Work model of alerting

● Alert server

Information about the sender’s IP addresses and the transmission time of a BOT that attempted to infect honeypots are provided for ISPs as alert information to identify the users of infected PCs. To incorporate that alert information into the regular work routine of ISPs, the information is downloaded from the proprietary server (alert server). (Note that the process of a sequence notification method, using mail for example, may be difficult to be regularized.)
ISPs are to download this alert information at optional timings, identify users based on this information, and then transmit alert mail to them. The URL of the measure site (disinfection distribution website) is inserted into the alert mail so that users can visit the site to download the appropriate disinfection tool.

● Tracking ID

Tracking IDs are created for the individual users of infected PCs, and not information such as names that identify privacy information. By using this ID, a user can obtain the disinfection tool for his/her own PC from the disclosed website of which the URL string includes the user's ID characters and/or numbers.
Users who visit the disinfection distribution website are collected and recorded in the form of tracking IDs. The visit records of users are also collected at certain points (tracking points) allocated at multiple locations on the website. By using these visit records (i.e., tracking records), it is easy to determine whether a user visited the website or downloaded the appropriate disinfection tool.

● Alert mail and measure site

ISPs identify the users of infected PCs based on IP addresses and the time stamps of alert information, and then transmit mail reporting BOT infection and the URL of the measure website.
On the disinfection tool distribution website, content is configured with disinfection tools, basic information on BOTs, and the disinfection tool execution procedure, as well as techniques to prevent the recurrence of infection. The content is prepared to give a visually friendly impression and intended to prevent basic questions from being asked, thus mitigating the user support work at ISPs. Moreover, thanks to the "go.jp" domain of the disinfection tool distribution website, the credibility of the website among users is enhanced.

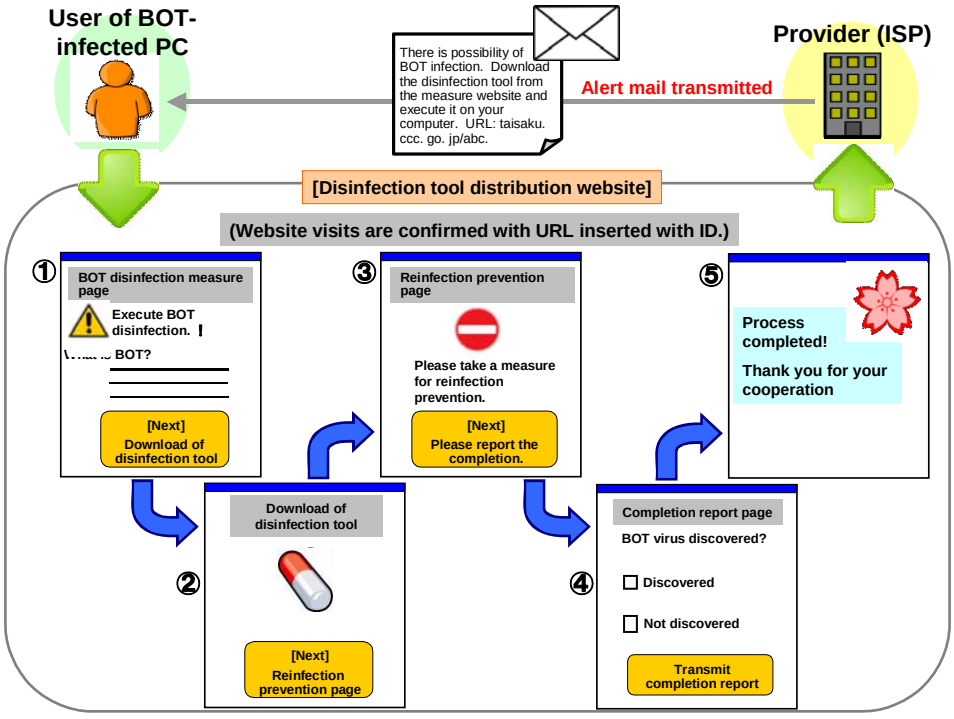

Fig. 2.3.3 Configuration of disinfection tool distribution website

● Mail transmission support

To support mail transmission work, the mail transmission application software prepared exclusively for this task is distributed to ISPs. This application software functions in collaboration with the server installed at the Center. By using this software, ISPs can select mail, for which form is patterned on a template, depending on such user attributes as individual or corporate entity and first infection or multiple infections, and also transmit mail at a predetermined interval.
The tracking history, such as regarding whether a user visited the measure website and downloaded a

disinfection tool, can be identified by using the tracking ID. An ISP can also refer to the identified results anytime.

● Execution cycle of alerting

The work cycle was designed and adjusted based on a liaison with related groups or organizations so as to minimize the transaction time from the capture of BOTs on a honeypot to providing a disinfection tool to users. As a result, disinfection tools are determined to be updated every week. In synchronization with such updates, alerts are transmitted to the users of PC infected with a BOT against which an updated disinfection tool enables disinfection.

However, if an attacking event is detected on a PC infected with a BOT against which a current disinfection tool is effective, the user is identified and alert mail transmitted immediately to eliminate the need to wait for any update.

2.3.3 Achievements

Transmitting alerts and downloading disinfection tools were counted as cooperative work with the project-participating ISPs for the period from November 2006 to the end of March 2007. As a result, 7,916 users were alerted and 1,861 users downloaded disinfection tools.

Alerts for verifying the effectiveness of these operations were sent out twice (with full-scale operation initiated based on the results of verification). Details are described below.

2.3.3.1 Results of alert verification

In the first alert verification, attacking events detected from November 25 to 30, 2006 were analyzed and identified with the senders. Then, seven ISPs participating in this project sent alerts to users from December 15. In the second alert verification, attacking events were detected from January 6 to 11, 2007, and eight participating ISPs sent alerts to users from January 15. The table below lists the numbers of users receiving alerts and downloads of disinfection tools. In addition, other results related to verification are shown below: ratio of visits to the disinfection tool distribution website by users who received alerts for their infected PCs, ratio of disinfection tool downloads, ratio of linking to Windows Update, and ratio of result reports made.

Table 2.3.1 Numbers of users alerted and disinfection tool downloads at alert verifications

	No. of users alerted	No. of disinfection tool downloads
First alert verification	105	31
Second alert verification	575	114

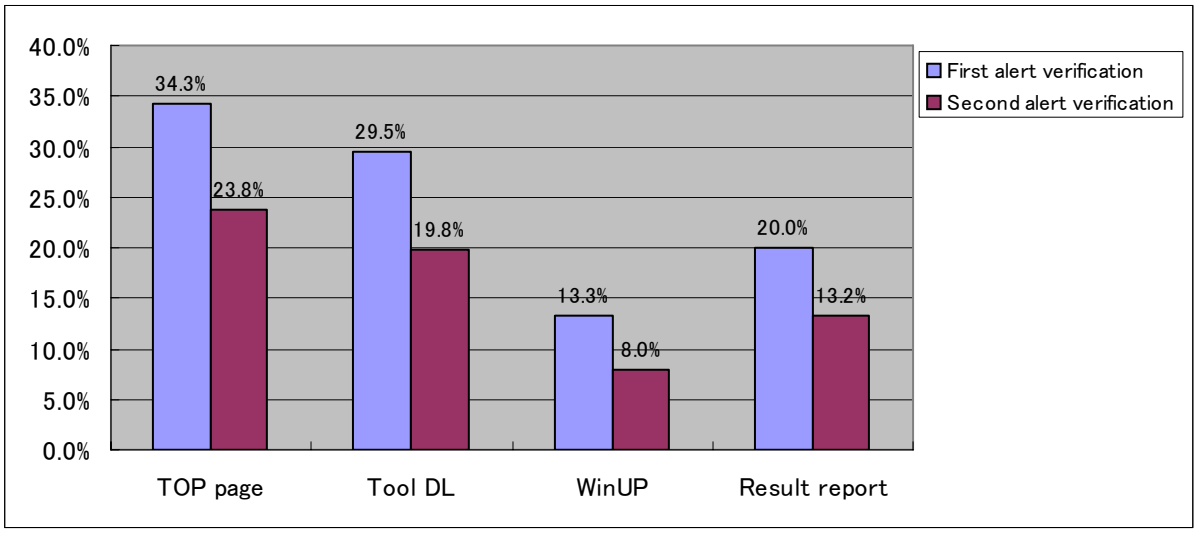

Fig. 2.3.4 Results of alert verifications

The ratio of visits to the top page of the disinfection tool distribution website was approximately 30%. To increase this number, it is necessary for users who do not access the website through repetitive transmission of alert mail, for example, to certainly recognize the fact of BOT infection. Applying certain tactics is also considered essential so that users take the fact of infection seriously, and even Internet beginners can easily take action.

The tendency of actions taken by website visitors is analogous for the first and second verifications. The results suggest that, although many visitors take action up to downloading the disinfection tools, many do not perform Windows Update, which is introduced on the next page of downloading or in the "completion report" found on the last page of the website to report the disinfection results. These results have been reflected in the design for full-scale operation of the measure website, as in aspects of the website structure or modified language.

2.3.3.2 Results of alerts in full-scale operation

In full-scale operation, the numbers of attacking events detected and users alerted for disinfection increased significantly due to an increased number of honeypots. In addition, based on the knowledge obtained from alert verifications performed twice, the transmission cycle of alert mail and design of the disinfection tool distribution website were modified.

- Alert mail: Alerts were sent multiple times to users who did not make a "completion report" on the measure website despite the transmission of alert mail.
- Measure website: Pages explaining the procedure for BOT disinfection were modified to plain expressions so that users could easily understand the content. Moreover, an additional function was mounted to enable checking of which user's infected PC communicated with a honeypot when making a visit.

In full-scale operation, ISPs began transmitting alert mail from February 19, 2007 against the attacking events detected on honeypots since February 5, 2007. The table below lists the numbers of users alerted about disinfection and disinfection tool downloads from the start of full-scale operation until the end of March 2007.

Table 2.3.2 Numbers of users alerted about disinfection and disinfection tool downloads in full-scale operation

	No. of users alerted	No. of disinfection tool downloads
Full-scale operation (Feb. 19, 2007 to Mar. 31, 2007)	7236	1716

In full-scale operation, the number of handlings was ten times higher than that during the pre-verifications.

The following chart shows the transition in the ratio of visits to the disinfection tool distribution website. The following steps were taken to prepare the chart: 1) alerting users began on February 19, 2007; 2) data was first collected on March 1 and the visit ratio calculated; and 3) data was later collected as the numbers of alerted users and website visits increased to calculate the approximate weekly visit ratio.

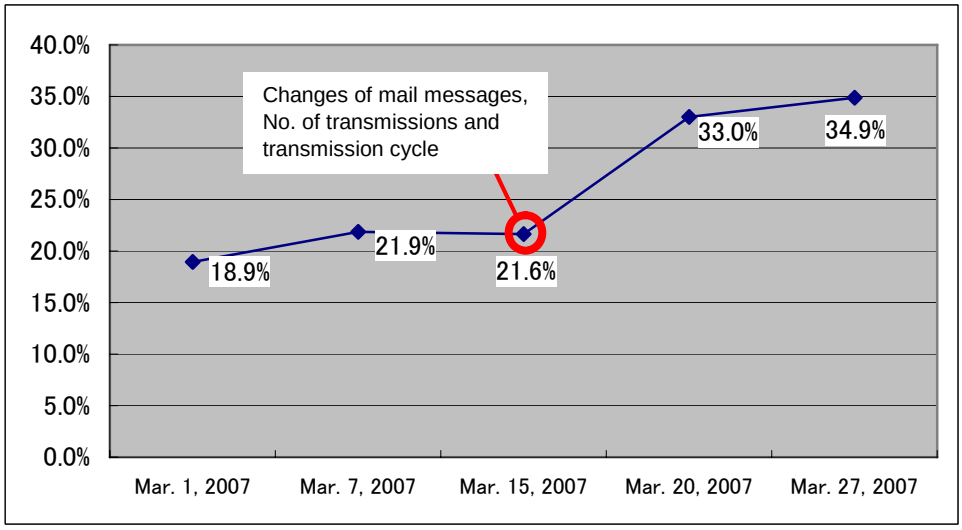

Fig. 2.3.5 Transition in ratio of visits to the disinfection tool distribution website

When data collection initially began on February 19, the visit ratio was below 20%, which is lower than that of the pre-verifications. Upon checking the status of alerting work at each ISP, the following was revealed: the faces of alert mail differed and the transmission cycles (intervals at which to retransmit mail to users who fail to take responsive action) were weekly at most ISPs but every three days at the ISP that showed the highest visit ratio. In order to improve the visit ratios, the operation style employed at the ISP providing the highest visit ratio was to be followed. Moreover, the face of alert mail was reviewed and modified for higher appeal. The visit ratio consequently improved to a level higher than that in the pre-verifications.

The following chart illustrates the visit ratios for the disinfection tool distribution website, as well as the ratios for downloading disinfection tools, linking for Windows Update, and making result reports.

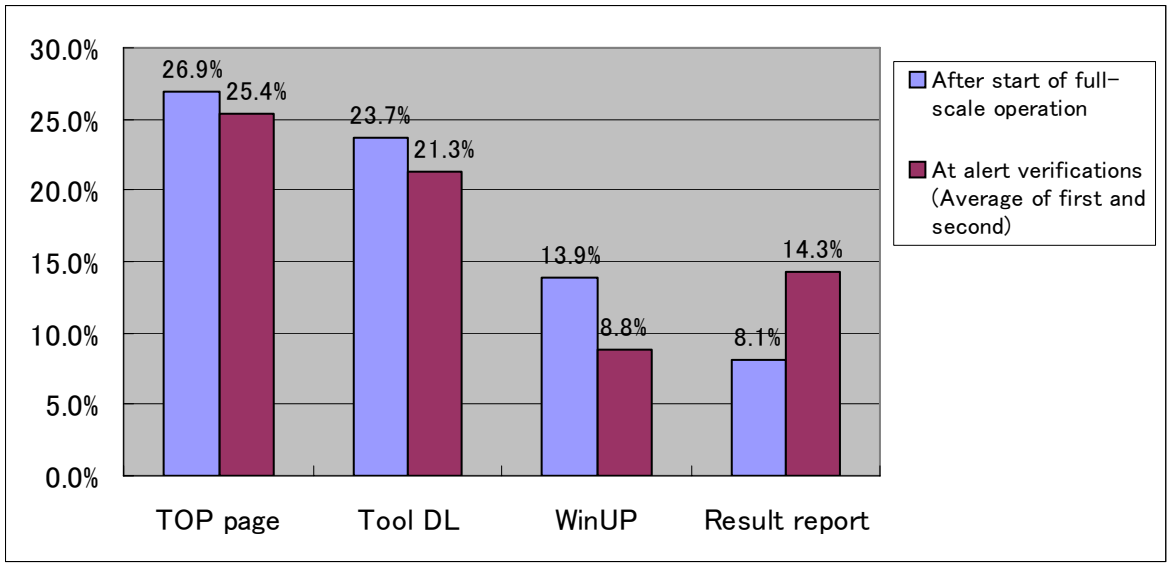

Fig. 2.3.6 Results of alerts during full-scale operation

In the pre-verifications of alerts, a single page explained the procedure for downloading disinfection tools, performing Windows Update, and making result reports. This was assumed the reason why the access ratio for Windows Update was slow in rising, since the result of a series of actions was reported immediately after a disinfection tool was downloaded without performing Windows Update. In full-scale operation, the procedure was split and restructured so as to be followed step-by-step as follows: disinfection tool download → Windows Update → result report. This was apparently very effective in drawing users toward Windows Update. In contrast, the result report ratio dropped. The reason is assumed to be that users gave up taking the next steps since Windows Update took considerable time or required rebooting.

In this project, specific disinfection tools are provided and explanations of detailed procedures offered on a website, while the role of alert mail for the users of infected PCs is limited to notifying them about BOT infection and drawing them to the website. This limitation was set because the conventional approach of sending mail to users explaining everything from tool distribution to detailed procedures may not improve their understanding of the mail's content, but instead may result in many questions being sent to the Center. No specific numbers are available to positively confirm such a possibility. However, upon hearing the opinions of participating ISPs, they feel that a much smaller volume of question mail will be received.

2.3.4 Future development

(1) Expanding the range of alerts

Since the number of users whose PCs are disinfected is only a small part of the total number of users whose PCs were BOT-infected as of the end of March 2007, expanding the range of reminding users by using alerts is an essential issue. Since BOTs are active in infecting IP addresses adjacent to those where they currently belong, cooperative work will be necessary with ISPs holding IP addresses not yet offered. Such work with ISPs of small organizational size will also be required for studying and finding solutions. Some transmission sources of infection activities still cannot be analyzed, while others transmit exploit codes as initial infection activities. Therefore, a study on sending alerts against such sources will be required in order to expand the range of alerts.

(2) Improving ratios of visiting the disinfection tool distribution website and modifying its structure
The visit ratio for the top page of the website has reached 35%. Still, it could be improved through the following process. First, the level of recognizing the techniques employed in this project should be raised so that users feel safer, since many users may now be hesitant to click the URL set in the mail because of phishing, for example. Secondly, regarding those users who visited the website but failed to follow the procedure after downloading a disinfection tool toward the steps of confirming the Internet environment to prevent infection again and making a "completion report," the website structure should be reviewed and modified to help users understand that downloading is not the end of the entire procedure to be followed.

(3) Contributing to a better understanding of how to prevent infection and recurrence
During full-scale operation, the number of users whose PCs were infected again accounted for about half of the total number of users of infected PCs, where PCs infected again are detected on honeypots as being re-infected by another type of BOT after the previous BOT was successfully disinfected with a disinfection tool. The reason for such recurrence is assumed to be a vulnerable Internet connection environment where, for example, a global IP address is directly terminated on a PC or a relatively weak OS is used. As measures against these problems, the use of a broadband router and performing Windows Update are strongly recommended. Overall, activities for enlightening users are being promoted in cooperation with other organizations and the mass media. Such activities will help curtail the expansion of not only the recurrence of BOT infection but also initial BOT infection.

3 Activity report - BOT program analysis group

3.1 Overview

The BOT program analysis group analyzes BOTs (analytes) captured by the BOT countermeasure system operation group and develops disinfection tools. Detailed analysis is conducted on certain analyzed BOTs using the static analysis technique, if needed.
The group also operates a system in which captured BOTs are provided for security vendors participating in this project as vendors to prevent infection.

3.2 Analysis

The following two types of analysis are conducted:

- Simple analysis: Intended to investigate analytes that current disinfection tools do not handle, in terms of types or information on files with respect to infection, and to create disinfection tools.
- Detailed analysis: Intended to conduct static analysis on analytes found in simple analysis to have potentially large effects on BOT trend analysis or future analysis techniques, in terms of weakness or behavior that BOTs may target to use, or techniques that BOTs currently use.

3.2.1 Processing flows of simple analysis and detailed analysis

3.2.1.1 Flow of simple analysis

This analysis is categorized as two processes: simple analysis conducted everyday including the preparation of a disinfection tool handling list, and the preparation of disinfection tools conducted every week.

1) Everyday work (simple analysis)

1-1) Preparation of handling list

(i) Obtaining analytes and related information from the BOT countermeasure system operation group

(ii) Extracting analytes for simple analysis depending on the criteria
The criteria are set on based on the following:

(1) Analytes not yet handled by anti-virus software (supplied by the disinfection tool developing business entity, and that supplied by two other business entities)
(2) Analytes not yet handled by anti-virus software supplied by the disinfection tool developing business entity (but may be handled by that supplied by two other business entities)
(3) Analytes attacking frequently

(iii) Preparing the handling list of analytes for which disinfection tools are reflected

(iv) Sending the handling list to the BOT countermeasure system operation group from the BOT program analysis group

1-2) Provision of extracted analytes for the BOT infection prevention promotion group

2) Work performed every week (preparation of disinfection tools)

(i) By Wednesday, analytes captured on Monday are subject to simple analysis and disinfection tools prepared.

(ii) On Wednesday afternoon, the disinfection tools prepared are provided for the BOT countermeasure system operation group.

(iii) By Wednesday, the BOT countermeasure system operation group establishes conditions under which the disinfection tools received can be distributed to ISPs whose members are the users of infected PCs, and discloses the tools on the Cyber Clean Center website so that users can download them.

(iv) On Thursday or later, ISPs send mail to the users of infected PCs, requesting BOT disinfection.

Figure 3.2.1 illustrates the process flow of simple analysis, disinfection tool preparation, and the provision of BOTs for the BOT infection prevention promotion group.

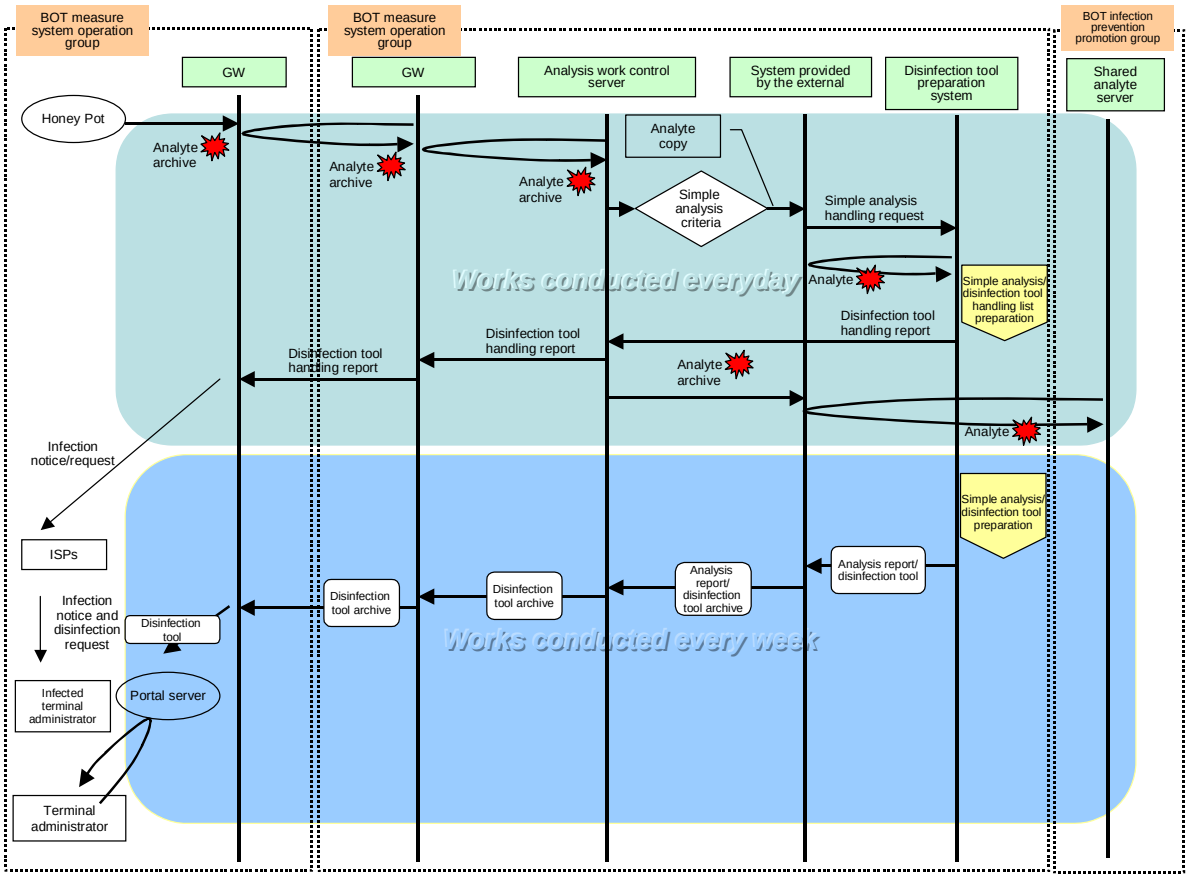

Fig. 3.2.1 Process flow for simple analysis

3.2.1.2 Flow for detailed analysis

(i) Extracting BOTs to be used as analytes from captured BOTs

(ii) Conducting detailed analyses on analytes extracted by the BOT program analysis group and disinfection tool developing business entities

Both types of work above are conducted at random intervals.

3.3 Static analysis

3.3.1 Study on static analysis

Static analysis is defined as analyzing the structures and specifications of programs subject to investigation, using reverse engineering (or reverse code engineering). In static analysis, since all program execution paths can be checked, the behavior of analyzed programs can be completely captured or various techniques used by malware are acknowledged. However, the disadvantage of static analysis is that it requires many work hours, since numerous assembly language instructions must be decrypted. Moreover, the analysis of reverse-assembled program codes requires considerable experience and broad knowledge about OSs, networks, and programming languages. There is no established technique available for static analysis, but engineers have developed their own effective techniques in a trial-and-error manner. Attempts have made to automate static analysis, though no fully automated method has yet to be announced. There are also many technical issues remaining to be solved. Thus, it is unlikely that fully automated static analysis will be available in the near future. The study on static analysis and new effective techniques must be continued, however, in order to counteract malware, which is becoming ever more sophisticated.

3.3.2 Trend analysis of BOTs

3.3.2.1 Background and purpose

It is essential for implementing security measures to understand the methodology adopted in attacks. Since the first BOT appeared several years ago, BOTs have advanced and become more intricate, while their techniques of infection, attack, and cover-up have changed. Without knowing the latest techniques of attackers, misguided measures could be taken.
For example, shutting down IRC communication is meaningless against a BOT transmitting commands using a method other than IRC communication.
Methods of analyzing traffic in networks or BOT programs, however, may be used to better understand the latest techniques employed by BOTs. The BOT investigation described below used the static analysis method.

3.3.2.2 Results of trend analysis

The following was discovered based on the static analyses of 20 analytes not duplicated in terms of names and families, and whose functions presumably differ from each other.

1) Common engine
Even if BOTs demonstrate completely different functions, the essential part of the BOTs may be considered the same. This may be true as the source codes of BOTs are disclosed on the Internet. Although more BOTs should be subject to static analysis in order to finalize the specifications, it is assumed that many BOTs employ a common engine with various functions added to them. Many currently prevalent BOTs could be categorized as several types, in terms of commonality of the essential part.

2) BOT commands

BOTs are incorporated with numerous commands, such as those for login or logout, connection to the IRC server, surveillance, and even attacks.

3) Weaknesses
BOTs utilize the following weaknesses of PCs, such as:
- The system is intruded via an unchecked buffer included in universal plug and play (UPnP) (MS01-059).
- Codes are executed due to buffer overrun in the RPC interface (MS03-026).
- There is a danger of random code being remotely executed due to the weakness of an unchecked buffer in plug and play service (MS05-039).
- Attacks of DCOMRPC using pipe¥epmapper

4) Packers
Many packers are freely available on the Internet. The goal of a packer is to change the structure of an executable program to hinder attempts to analyze it. At least 15 different types of packers are used for BOTs.

5) Difficult to read
One BOT makes itself difficult to be read by modifying the API.

6) Unpack technique
Unpack routines employ anti-debugging techniques. Memory access invalid on offset 0 (zero) is one of the anti-packing techniques used in unpack routines. This technique has been used relatively frequently in recent packers.

7) Concealed as a variant
In the latest malware including BOTs, codes may be regularly modified based on changes in hash values. However, there is a part of malware that reportedly does not employ any code modification function. To escape detection by anti-virus software, concealing BOTs as a variant may be attempted by requiring more analysis effort.

8) Component-based BOT
One report describes that there is now more malware including BOTs, made component-based in a single function or per function, and downloaded from the Internet to cause infection.
Such malware is called a “DOWNLOADER.” A single DOWNLOADER can infect a system with multiple pieces of malware, extend the functions of malware, and change or modify malware. These features are incorporated to make malware difficult to quickly identify so that it can escape disinfection. When certain components are disinfected but a DOWNLOADER remains alive, infection may reoccur.

3.4 Future development

During FY 2006, this group worked to enhance analyzing capability for project steering and establish a preparation scheme of analysis work. This scheme was successfully established in the scope initially intended, but issues have surfaced and events changing over time require continuous efforts to be made. This project is responsible for the bulk flow including the portions from capturing BOTs up to the application of disinfection tools, where the operational stability of these portions in the flow is crucial.
In FY2007, top priority is placed on enhancing the operational stability of the current scheme, and an organizational structure will be sufficiently built up to allow the tuning of the scheme and disinfection tools

in response to changing events. Regarding detailed analysis, efforts are being made not only in analyzing individual BOTs but also in trend analysis and a long-term study on analytical techniques.
As of the end of FY2006, the following necessities were recognized with respect to the tuning of disinfection tools or extension of functions, which are targeted to be achieved in FY2007.

(i) Addition of setup function for disinfection tool expiration date
(ii) Addition of setup function for standard search mode corresponding to types of analytes
(iii) Addition of tracking function for disinfection results
(iv) Response to Rootkit
(v) Reinforcement of platform corresponding to disinfection tools

4 Activity report - BOT infection prevention promotion group

4.1 Overview

The BOT infection prevention promotion group in this project is responsible for reinforcing measures against BOT infection and broadly preventing recurrence among general users in cooperation with security vendors (hereinafter referred to “infection prevention measure vendors”).
More specifically, this group provides analytes collected during various activities in this project to the infection prevention measure vendors so that they can reflect the analytes in the pattern files of their commercially available anti-virus software. When users update their anti-virus software for these pattern files, the files can detect and disinfect the BOTs collected in this project, resulting in improved security.

4.2 Infection prevention measure vendors

Vendors participating in this project are legal entities that follow strict control regulations on analytes, have departments assigned to conduct analysis in Japan, and possess extensive experience in the supply and services of countermeasure software in Japan. This group, together with these infection prevention measure vendors, assumes the role of promoting infection prevention activities on PCs and other equipment owned by users.

List of participating infection prevention measure vendors
- Microsoft Corporation
- Sourcenext Corporation
- Trend Micro Incorporated
- McAfee Incorporated
- Symantec Corporation

4.3 Achievements

The table below lists the records on how analytes were reflected in pattern files by the infection prevention measure vendors as of the end of March 2007. The percentages indicate ratios of the number of occasions of reflection against the total number of occasions on average among all the project-participating vendors.

Table 4.1.1 Records on how analytes were reflected in pattern files

Occasions where analytes were provided by the BOT program analysis group, and reflected in pattern files of the infection prevention measure vendors	48.2%
Occasions where the vendors handled their own pattern files for a specific type of analyte before the BOT program analysis group provided the same type of analyte	49.4%
Occasions where analytes were not reflected in pattern files	2.4%

1) The total number of types of analytes provided by this project in the period from December 2006 to the end of March 2007 is equivalent to “100%.”

2) The average percentage over the vendors for analytes provided by this project is 48.2% as listed in the table. This indicates that the analytes collected were sufficiently utilized. This is one achievement of this project.

The participating infection prevention measure vendors currently occupy more than 90% of the total domestic market share. The result of 48.2% should be considered a significant contribution to preventing the infection of PCs owned by general users.

4.4 Future activities

The group will continue fulfilling its role in this project by strictly controlling the analytes collected, as well as enhancing the reflection of those analytes in the pattern files of anti-virus software sold by the vendors through cooperative work with those vendors.

5 Summary

The BOT network measure project is the first attempt made in Japan and among the few attempted in the world to eradicate BOT-infected PCs, for which cooperative work between the Ministry of Internal Affairs and Communications, the Ministry of Economy, Trade and Industry, other governmental organizations related to the project, and business entities began in December 2006. Public awareness of BOTs has since been improved. This may be attributed to efforts made by this project, as well as reporting by the mass media of the project's activities and achievements, where many users of BOT-infected users have been alerted about infection and actually disinfected BOTs. The project must continue to exercise ingenuity to rouse the attention of even more users against BOTs, since there are still many users of infected PCs. Technical innovation to ward off the threats of BOTs is also expected, as BOTs continue to evolve day by day. Furthermore, activities conducted from the perspective of cooperation with overseas organizations must be studied, since the threat of BOTs also exists outside Japan. This project will continue to actively contribute to establishing a safer and more secure Internet society.