The Fight Against the Threat from Botnets

Report on the activities of the

Cyber Clean Center (CCC)

August 31, 2010

Cyber Clean Center

Anti-Botnet Project

https://www.ccc.go.jp

(Blank Page)

Contents

1. Introduction

With the widespread proliferation of the Internet, there are a growing number of problems caused by unauthorized accesses and malicious software. There are various categories of malicious software, such as viruses, Trojan horses, spyware, botnets, etc. They are collectively termed “malware.”

Botnets, in particular, are distinctive in that they infect personal computers (PCs) without the users being aware of them. Recently we have often seen the generation of many subspecies over a short period, and which cannot be detected or disinfected by anti-virus software. This makes it difficult for PC users to take active countermeasures. It is becoming more important for the government to propel anti-botnet measures by collaborating with Internet Service Providers (ISPs), security software and service vendors, and organizations addressing computer security, rather than leaving users to undertake the implementation of safety provisions.

Against this background, with the intention of reducing the number of botnet-infected computers as close to zero as possible, the Cyber Clean Center (CCC) was established as part of a joint project by the Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy, Trade and Industry (METI) in fiscal year 2006. This report summarizes the activities of the three groups under the CCC: the Bot Countermeasure System Operations Group, Bot Program Analysis Group, and Bot Infection Prevention Promotion Group. This is a wide-ranging report that includes techniques and hints on operating and constructing computer systems that have not been released in previous results reports.

2. Background and summary of activities

2.1. What is a botnet?

Today the Internet is an important piece of infrastructure that supports our everyday life. It is used for various purposes by both the public and private sector, and by a wide demographic from children to senior citizens. The Internet is now an indispensable part of daily life. Coinciding with this, there is growing number of diverse criminal activities that are abusing Internet resources.

Malware is a newly coined term meaning “malicious software.” It has a broad definition and is categorized by the function or type of infection: viruses, worms, Trojan horses, Botnets, etc. A botnet refers to a number of software agents that are remotely controlled by the commander software, called the “herder,” to perform various harmful acts, such as Distributed Denial of Service (DDoS) attacks, spamming, and phishing.

Infectious attacks and botnets

In general, bots attempt to infect PCs on an adjacent network (or a PC whose IP address is near the IP address of the bot). If a target PC has an exploitable security vulnerability, it may be infected. A group of infected PCs, sometimes called “zombie PCs,” connect themselves to a relay server called a Command-and-Control (C&C) server and form a network called a botnet. A botnet may comprise of several thousand to several tens of thousands of bots.

Since a PC infected with a bot (bot-infected PC) seldom displays signs of suspicious behavior, the user is usually unaware of the infection. The herder then instructs the infected PCs to send spam mails or perform DDoS attacks by sending various commands through the C&C server, all unbeknownst to the user.

Rather than prank activities such as displaying fireworks on the PC screen or deleting files on the hard disk, which have often been seen on virus-infected machines in the past, botnets are typicallyused for information fraud by criminal organizations. The mechanism of how a botnet is formed is shown in Figure 2-1. An example of a crime committed with bot-infected PCs that are remotely controlled by the herder is illustrated in Figure 2-2.

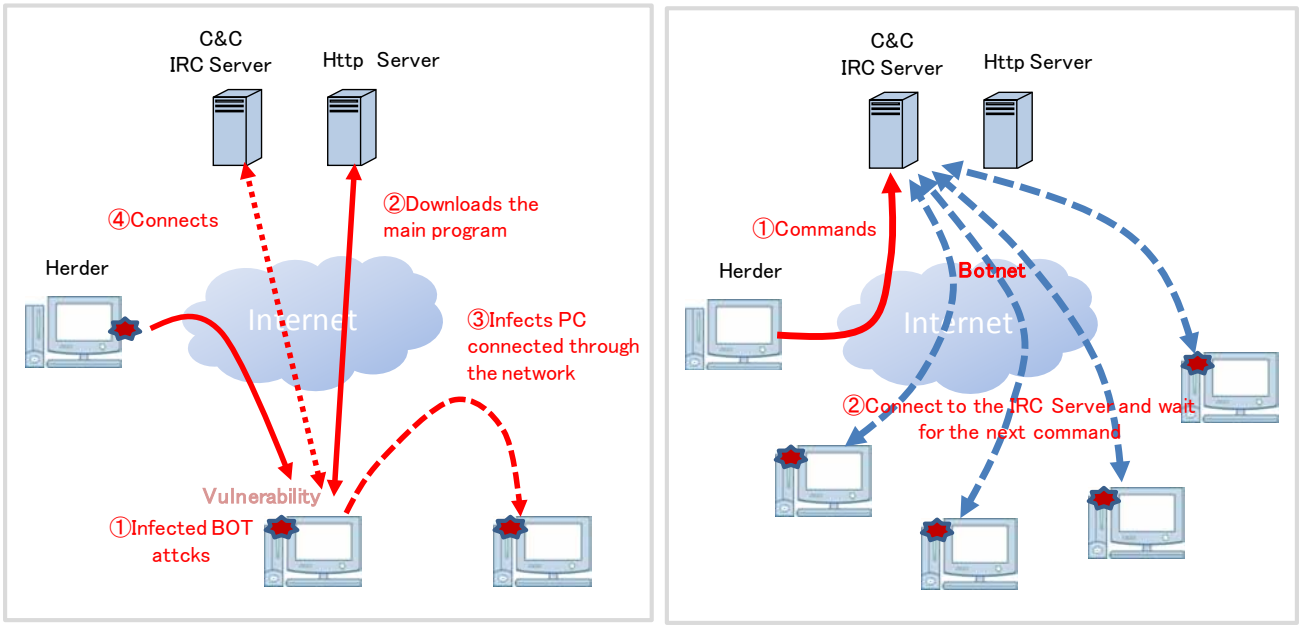


Figure 2-1: How a botnet is formed

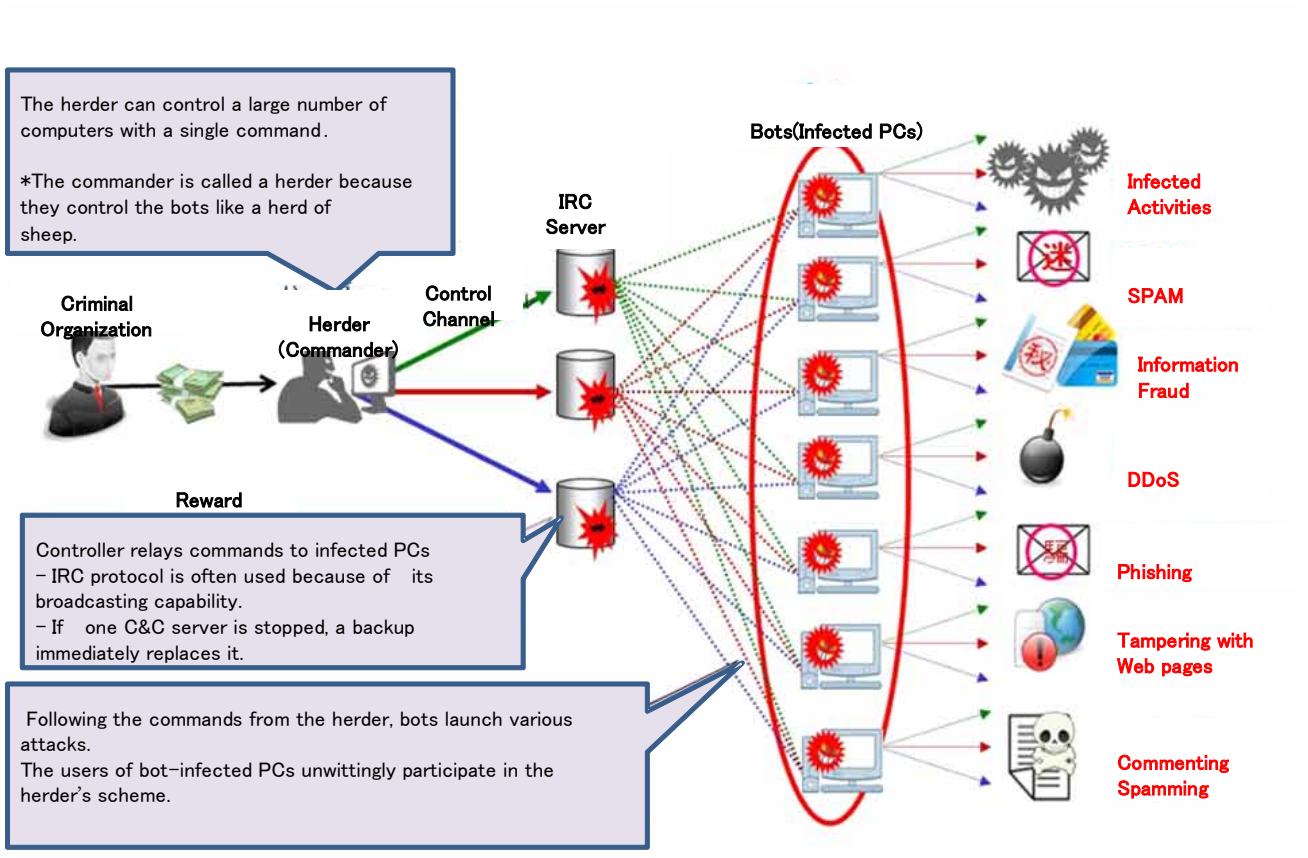


Figure 2-2 Example of criminal activity using a botnet

2.1.1. Characteristics of a botnet

A botnet has the following main characteristics:

(1) Infected PCs can be manipulated to commit fraudulent activities

The major purpose of a computer virus is to infect PCs while that of a botnet is to make use of the infected PCs to perform malicious activities.

(2) Infected PCs become the guilty parties

PCs infected with a bot (bot-infected PCs) are not only the victim of information fraud, but also may become guilty parties when they are controlled by the herder to act as sources of Denial of Service (DoS) attacks or as senders of spam mail.

(3) PCs remotely controlled by the herder

Bot-infected PCs are remotely controlled by the herder and can execute various commands issued by the herder.

(4) Undetected by anti-virus software

A bot often involves the generation of variants in a short period, which cannot be detected or disinfected by anti-virus software. Once a bot infects a PC, it may disable updating of installed anti-virus software.

(5) Easy to add further functions

Since a group of bot-infected PCs form a network called a botnet, they can download new bots and add new functions under the control of the herder. These functions also enable the bot itself to change so that it cannot be detected by anti-virus software.

2.1.2. Bot infection status

The existence of bots first observed in 2002. Since about 2004, the increase in botnet infections has been noticeable. According to a survey conducted by Telecom-ISAC Japan and JPCERT/CC in June 2005, the PCs of 400,000−500,000 users out of the total 20 million broadband users in Japan are infected with bots (an infection rate of 2.0−2.5%).

2.2. Need for countermeasures

As indicated in 2.1.1Characteristics of a botnet , bots infect PCs without users being aware of them, which further increases the damage.

To prevent the spread of bot infections, it is essential that:

- ISPs or other organizations find infected PCs by detecting infection attack events.
- ISPs or other organizations notify the users of infected PCs and request them to take the necessary measures.
- Users of infected PCs remove bots and take countermeasures to prevent re-infection.

However, since PC users do not necessarily have adequate knowledge of anti-bot measures and

many ISPs have not created anti-bot schemes, the reality is that anti-bot measures are difficult to carry out by PC users, who need to pay for the extra cost, and ISPs, who have limited resources.

For this reason, MIC and METI teamed up with information security organizations, ISPs, and security vendors to establish the Cyber Clean Center (CCC) as a national project. The CCC started activities in December 2006.

2.3. Overview of the CCC

The CCC was established by MIC and METI for the purpose of reducing the number of botnet-infected computers to as close to zero as possible, and has been active since December 2006.

The CCC is a five-year project from fiscal year 2006 to 2010. Along with Telecom-ISAC Japan, JPCERT/CC, and IPA, as of April 2010 76 ISPs, 7 security vendors who develop and sell anti-virus software, and many other vendors and research institutes were working together to promote anti-bot activities.

2.3.1. Anti-bot approaches

There are several approaches to dealing with bots. The approach adopted by the CCC is to identify bot-infected PCs, then notify the users of those PCs.

Before the CCC started its anti-bot activities, the following three approaches were discussed.

(1) Apprehend herders

In some countries, efforts are under way to reduce the damage perpetrated by bots in co-operation with law enforcement to arrest the herders who control botnets. However, detecting and intercepting the communications by herders who are remotely-controlling botnets is technically difficult. Additionally, it is infeasible in Japan because this would be an infringement of the confidentiality of communications under Japanese law.

Even if such activities were allowed, there would be other obstacles. Since most herders are overseas, it is difficult for a single country to take measures against them. Moreover, even if the authorities did arrest the herder and stopped the botnet, the bot-infected PCs would still exist and continue infecting other hosts.

(2) Disable C&C servers

The next approach is to find and disable C&C servers and deactivate their botnets. C&C servers are typically less difficult to identify than the herders themselves. However, since most C&C servers are overseas, it is difficult for Japan alone to stop them.

Moreover, when a C&C server is detected and disabled, the herder can simply set up another C&C server. Therefore, it is difficult to completely exterminate a botnet in this way.

Instead of terminating the C&C server, one can disrupt the communications between bot-infected PCs and the C&C server. However, this is infeasible in Japan because it is an

infringement of the confidentiality of communications under Japanese law. In addition, using either method (i.e. disabling the C&C server or breaking communications with the C&C server), bot-infected PCs still exist and can continue their infection attacks.

(3) Deal with bot-infected PCs

A PC infected with a bot attacks neighboring IP addresses in order to spread the infection. This approach installs honeypots (i.e. decoy PCs) covering an IP address range and collects the attackers' IP addresses and the time of the attack. Based on this data, each ISP determines who was connected at that time, and identifies the user and ID. The ISP then issues a warning asking the user to remove the bot from his or her PC.

Directly notifying the user of each bot-infected PC and encouraging disinfection may reduce the number of infected PCs in Japan. This activity may also help educate users of infected PCs by providing information on security and improving computer literacy.

As stated above, the approach to herders and the approach to C&C servers are technically and legally infeasible. Even if these approaches were implemented, the bot-infected PCs would still exist in Japan and continue infection attacks, expanding infections, and are therefore not comprehensive solutions. Anti-bot approaches, measures, and problems are listed in Figure 2-3.

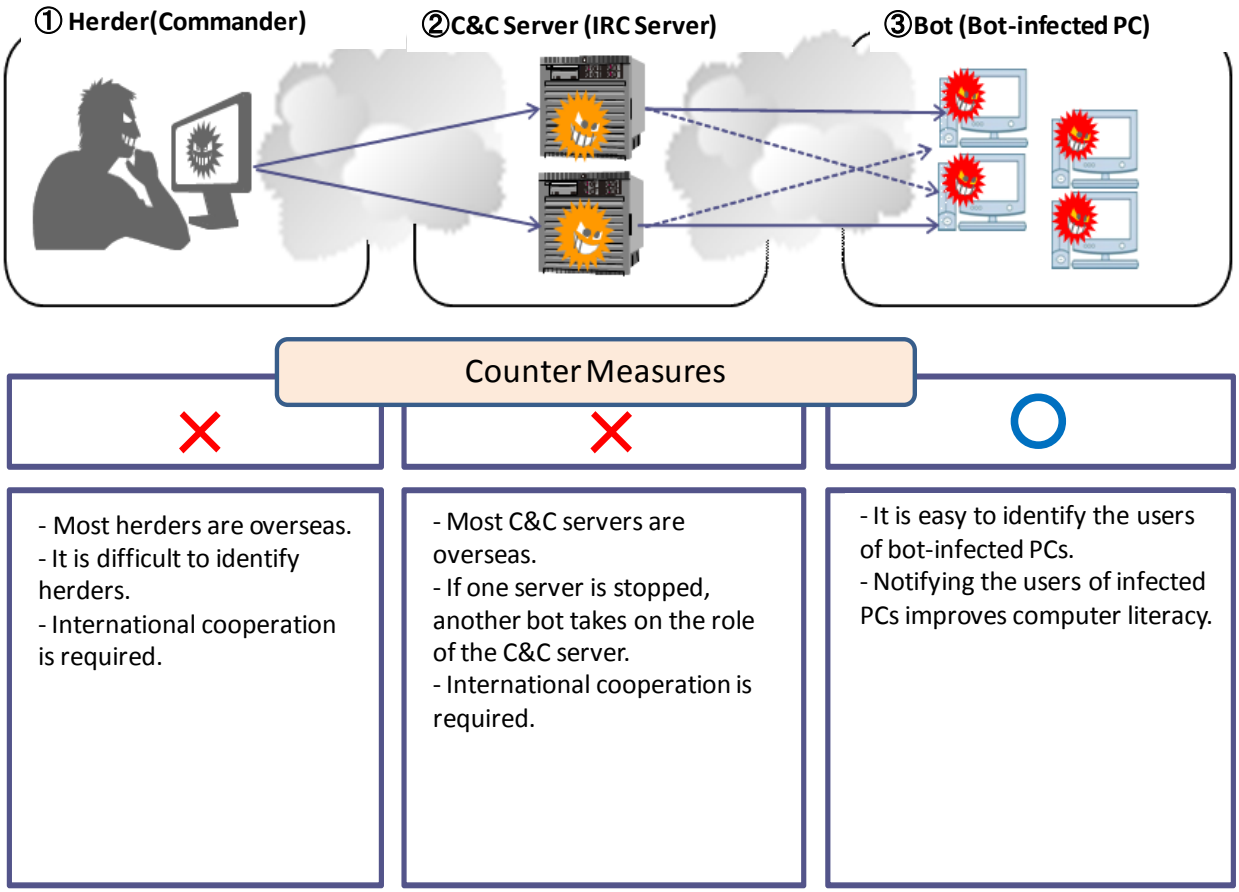


Figure 2-3: Anti-bot approaches

For the above reasons, the CCC has adopted the approach to address bot-infected PCs. We are working on identifying infected PCs and giving warnings, as well as conducting campaigns to educate users about proper security measures.

2.3.2. Concept of anti-bot measures

With the aim of reducing the number of botnet-infected computers to zero, the CCC is carrying out activities with three specific concepts in mind:

(1) Identifying bot-infected PCs
(2) Providing the users of infected PCs with specific countermeasures
(3) Preventing those PCs from being re-infected with bots

2.3.3. Operations and roles of the CCC

Under the Cyber Clean Center-Steering Committee (CCC-SC), the CCC consists of three groups covering different purposes and conducting daily activities. The operational framework of the CCC is shown in Figure 2-4.

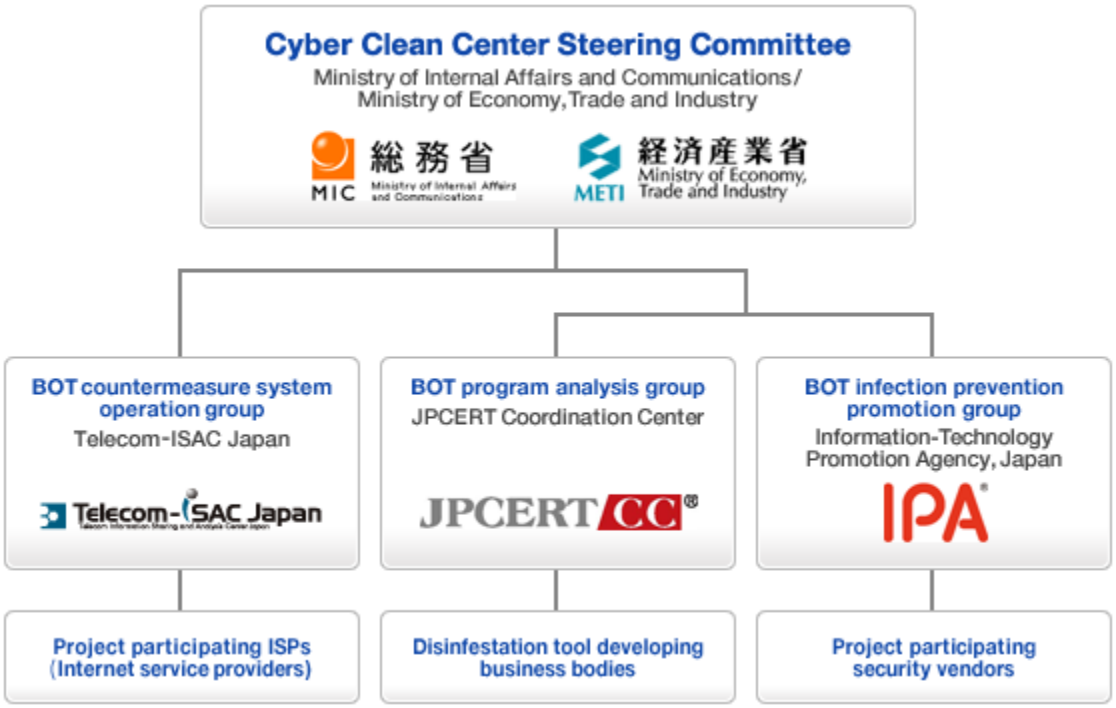


Figure 2-4: CCC operational framework

(1) Bot Countermeasure System Operation Group (Telecom ISAC Japan)

The Bot Countermeasure System Operation Group operates the main systems of this project, including the Honeypot System and Warning System to collect and analyze bots, and notifies users of bot-infected PCs through the ISPs participating in the project. With the aim of countering

the new thread of bots and implementing effective measures, the group collaborates with security vendors to conduct surveys on the latest malware trends.

(2) Bot Program Analysis Group (JPCERT Coordination Center)

The Bot Program Analysis Group analyzes the characteristics and technology of the bot samples collected by the Bot Countermeasure System Operation Group. This group works with disinfection tool developers to provide the “CCC Cleaner” disinfection tool. They also study effective analysis methods and cooperate with security vendors to develop countermeasure technologies.

(3) Bot Infection Prevention Promotion Group (Information-Technology Promotion Agency, Japan)

The Bot Infection Prevention Promotion Group maintains bot samples collected by the Bot Countermeasure System Operation Group. The samples are quickly provided to security vendors so that they can reflect them in the creation of pattern files. Therefore, the users of anti-virus software can disinfect unknown bots before their infection spreads. This group promotes infection prevention by reducing the risk of infection.

2.3.4. CCC workflow

The workflow among the Bot Countermeasure System Operation Group, Bot Program Analysis Group, and Bot Infection Prevention Promotion Group are shown in Figure 2-5.

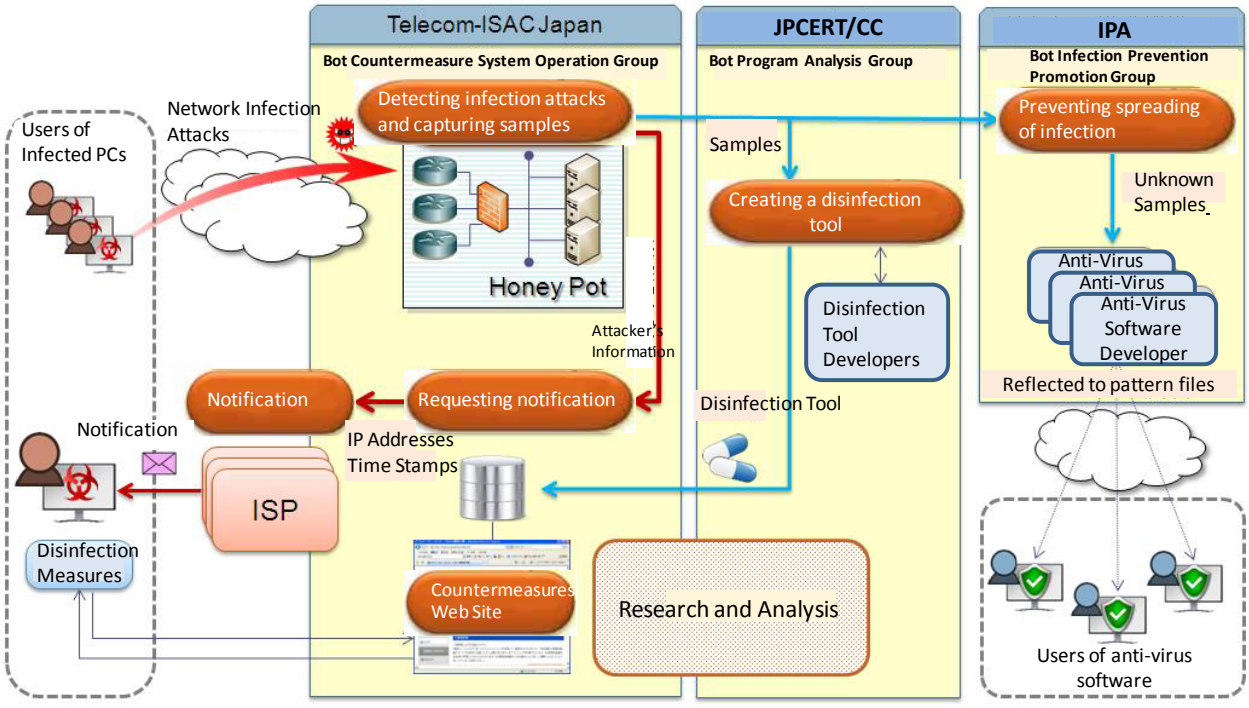


Figure 2-5: General workflow

The major roles of each group are listed in the following table.

Bot Countermeasure System Operation Group	Finding bot-infected PCs and notifying the users	Detecting infected PCs and warning users
Bot Program Analysis Group	Providing specific countermeasures	Developing disinfection tools
Bot Infection Prevention Promotion Group	Preventing the spread of infection	Promoting infection preventing activities

3. Activities of the Bot Countermeasure System Operations Group

The Bot Countermeasure System Operations Group collects the IP addresses of PCs infected with bots using the Honeypot System. The group then notifies the users of the infected PCs through the ISPs participating in the project.

The bots and other malware collected by the Honeypot System are sent to the Bot Program Analysis Group where they are used to update the pattern files of the CCC Cleaner. They are also supplied to security vendors through the Bot Infection Prevention Promotion Group and reflected in the pattern files of their anti-virus software.

The following sections provide discussions on the methods, specific activities, and accomplishments in regard to user notifications. System details are covered in the section on specific activities.

3.1. Discussions on anti-bot measures

3.1.1. Identifying the users of bot-infected PCs

One of the important things when identifying the users of bot-infected PCs and notifying them is that we can inform the users of bot infection with certainty. Particularly when an ISP warns the users of bot infection, it is necessary to clarify the basis on which the ISP is issuing its warning.

Before the project started, the warnings sent from ISPs to the users of infected PCs were mostly based on reporting to ISPs on mail attachment viruses, as well as attacks from Blaster, Sasser, and other viruses which the victims could easily recognize as virus attacks.

In contrast, the users of PCs infected with bots by infection attacks are seldom aware of infection. Even if they noticed an infection, it would be difficult to identify and prove through which IP they were attacked and infected. Moreover, reports to ISPs are not easy to verify as correct.

Therefore, detecting infection attacks from bot-infected PCs at an early stage, notifying the users of those PCs, and asking them to disinfect and take countermeasures are urgent matters. In this project, we reviewed the methods for effectively detecting infection attacks from many bot-infected PCs.

A bot launches infection attacks using the vulnerabilities of PCs on the IP addresses neighboring to the IP address used by the bot-infected PC. Therefore, we installed honeypots on such IP addresses, which enabled us to collect attacks efficiently. To cover the IP address ranges when there are many infected PCs, we have prepared band ranges with the assistances of a number of ISPs.

The Bot Countermeasure System Operations Group maintains multiple honeypots to record the attacks from IP addresses (those used by the infected PCs) and time stamps, which serve as clues to identify the users of the infected PCs.

Honeypots are broadly divided into two types: Low-interaction honeypots[1] that emulate certain operating systems (OSs) and software, and high-interaction honeypots[2] that use a "real" OS. This project decided to implement high-interaction honeypots. Since they use "real" OSs, it is possible to infect the honeypots in an environment similar to that the bot-infected PCs are running.

High-interaction honeypots can collect the entire bot program as well as observe the infection attacks from bot-infected PCs. Obtaining the entire bot is significant from two viewpoints.

First, capturing a bot generated by infection attacks from bot-infected PCs provides the users of the infected PCs with proof that their PCs are infected with a particular type of bot. This enables ISPs to warn PC users with confidence.

Secondly, it is possible to create a CCC Cleaner that corresponds to the collected bot. If the CCC Cleaner does not support the bot collected, the warned users have no means to disinfect the bot. In such a case, a pattern file is created immediately, and when it is reflected in the CCC Cleaner, ISPs issue a warning to the users.

3.1.2. Warning to bot-infected PC users

Once the users of bot-infected PCs are identified, a warning is issued to those users.

Specific procedures includes an announcement method that calls the attention of all customers of an ISP by e-mails and Web site announcements, and an individual method that warns each user of an infected PC by e-mail, telephone, or regular mail.

The announcement method is relatively simple from the viewpoint of operating the warning system. However, warning e-mails target every user—no matter whether a user's PC is infected with a bot or not. Such warnings are not necessarily effective in ensuring that the users of infected PCs take countermeasures. Similarly, displaying warning announcements on the top page of the Web site has only a limited effect. Very few users actually visit the web site describing the necessary measures (i.e. countermeasures Web site).

The individual method sends a personalized massage to each user of the infected PCs. It is more effective in ensuring that the users read the messages and recognize that their PCs are infected.

Accordingly, we have introduced the individual method and chosen e-mail as the means to carry warnings.

Conventional warnings on virus infections that ISPs have given previously are in the form of an e-mail with a long explanation describing countermeasures. However, there are limitations in explaining things in an e-mail and letting the users take proper measures. Therefore, we use a method that describes specific procedures, which are sometimes difficult to express in text form, on the Web site, together with

---

[1] Low-interaction honeypots emulates major vulnerabilities of the Microsoft operating systems. They can quickly detect attacks and process them. They record the time, communication protocols, source IP, source port, destination IP, destination port, and exploit type for each attack.

[2] High-interaction honeypots uses a Microsoft operating system as a virtual operating system, which is actually infected. The system is reset at regular intervals and various types of malware, such as the entire bot program that is downloaded after infection can be captured. They record the times, communication protocols, source IPs, source ports, destination IPs, destination ports, file sizes, SHA-1 hash, file names, and directory names. They can also identify the users of the attacking bot-infected PCs.

illustrations, so that users with various levels of computer skills can fully understand.

A warning e-mail issued by the ISP includes the warning text and the URL of the countermeasures web site with a tracking ID to identify the user. The tracking IDs enable the ISP to monitor each user and whether the countermeasures have been implemented. As warning e-mails include the URL of the countermeasures Web site, they might be taken as fraudulent and examples of phishing. ISPs and other organizations themselves recommend avoiding clicking URLs in an e-mail as a protection against phishing. Therefore, the method used to assure the credibility of such warning e-mails is important. To resolve this matter, the sending address comes from the infected user's ISP, the text includes a statement that this is a national project, and the URL is in the "go.jp" domain which indicates it belongs to the Japanese government. In addition, the target web site has a web site certificate from a third-party Certification Authority, and the communication is protected with SSL.

3.1.3. Effective and efficient methods of warning

When an ISP sends warning e-mails to the users of many bot-infected PCs, it is necessary to consider the burden on customer support. We also discussed how to send a large number of warning e-mails efficiently and how to support each user who has received a warning e-mail, such as re-sending messages depending on the user's progress in taking countermeasures. Such a discussion is important because the warning activities require the cooperation of ISPs and through these discussions we can estimate whether the project will enlist their cooperation.

In practice, we provide ISPs with information on the progress in taking countermeasures against each bot-infected PC user , the progress management system that maintains the users' infection history, and the warning system that facilitates sending warning e-mails based on the progress information and infection history.

The warning system offers an environment in which ISPs can create the text of the warning e-mail with little effort and the sending interval can be automatically adjusted.* The following action and the next state have been defined in advance according to the current state and event. The process runs following the flow determined in advance. This enables efficient operations and reduces the burden placed upon operators.

As a means for the users of infected PCs who have received a warning to disinfect the bot, we decided to provide the CCC Cleaner, a tool for removing bots. We provide this tool because it is simple to use for everybody, does not require installation, and does not conflict with anti-virus software.[3]

If a PC user has not installed anti-virus software, it is important to install it so that his or her PC is protected at all times. However, if the PC is infected with a bot, the bot may tamper with the hosts file and registry, stop certain processes, and inhibit raising the security level. It follows that to install anti-virus software properly, it is necessary to remove the bot beforehand.

If the description on the countermeasures Web site is vague or difficult to understand, many inquiries

[3] During the early part of the project, there were many bots that could not be detected by anti-virus software. After the software was installed the PCs could be left infected. This is why we considered the conflict with anti-virus software.

will be made to the ISPs, which will impose an excessive burden on their customer support section.[4] To avoid this, we have provided a web site explaining the necessary measures that users with various levels of computer skills can understand, which will ease the participation requirements of ISPs in anti-bot activities.

* Specifically, it is possible to adjust the interval of sending warning e-mails, select the text according to the number of resends, and other automatic adjustments according to parameters such as user type (corporate or individual), first or repeated infection, etc.

3.2. Specific activities

The warning activities of the Bot Countermeasure System Operations Group are broadly divided into three types.

(1) Collecting bots

Install a honeypot system to collect bots, which are handed over to the Bot Program Analysis Group.

(2) Identifying the users of bot-infected PCs

The infection log (IP address, date and time) of a bot collected by the honeypot system is provided to the pertinent ISP so that they can identify the user who used the listed IP address.

(3) Warning the users of bot-infected PCs

The ISP sends a warning e-mail to the user of a bot-infected PC. It includes the URL of the countermeasures Web site that describes the procedure for disinfecting bots (Figure 3-1). The URL contains a character string (tracking ID) unique to each user, with which the ISP can keep track of each user whether he or she has implemented countermeasures.

The user of an infected PC accesses the countermeasures web site, reads the description on the “risk of bots”, performs Windows Update and downloads the CCC Cleaner, and then by using the Cleaner removes the bot. After that, the user is recommended to install anti-virus software. Finally a “completion message” entered from the countermeasures web site is sent to the ISP. The Bot Countermeasure System Operations Group checks on the progress in taking countermeasures of each user by observing the procedural steps taken.

[4] Providing consultation on disinfecting bots is generally not included in the range of the support service by ISPs.

Figure 3-1: Countermeasure web site

To increase the efficiency of warning activities, the Bot Countermeasure System Operations Group has designed a workflow and built a system for performing it effectively. The next chapter describes the workflow and the system, related problems, and solutions.

3.2.1. Workflow and system

The workflow for performing warning activities efficiently is shown in Figure 3-2.

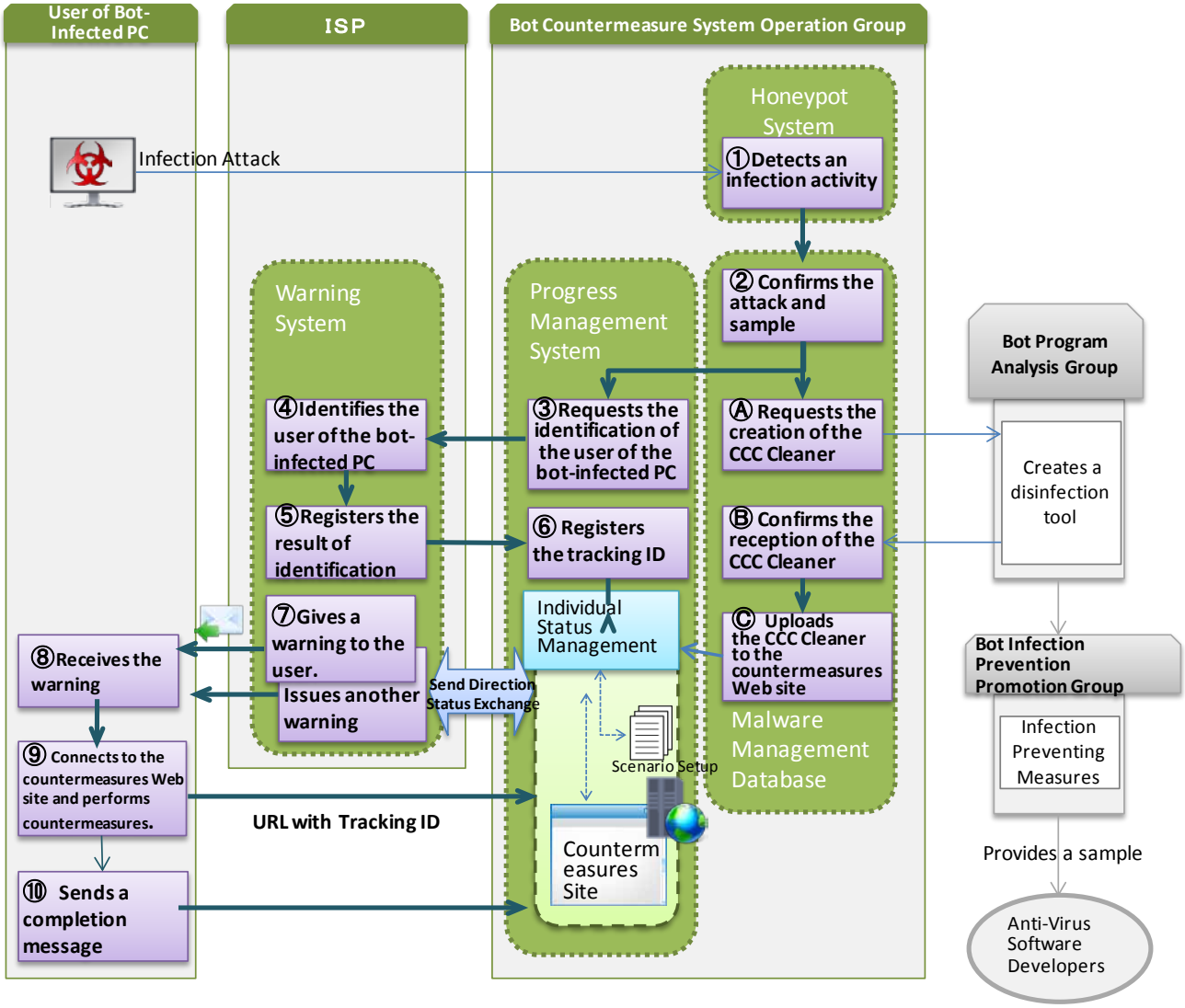


Figure 3-2: Workflow

The workflow is as follows:

① Detecting an infection attack (Bot Countermeasure System Operations Group)

The Bot Countermeasure System Operations Group uses the honeypot system to observe the communication from the bot-infected PC, and collect the bot with the attacker's IP address and time stamp of the infection attack (attack event).

② Confirming the attack event and sample (Bot Countermeasure System Operations Group)

The Bot Countermeasure System Operations Group obtains a bot sample collected by the honeypot system and related information on the attack event. The bot sample is matched against existing samples to determine whether it has already been registered. If it is a new sample, it is scanned with anti-virus software to check whether it is detected. The attack event is registered to the database.

(A) Requesting the creation of the CCC Cleaner (Bot Countermeasure System Operations Group)

The new sample, the number of attacks, and the support by anti-virus software checked in (2) are handed over to the Bot Program Analysis Group where an update to the CCC Cleaner is created.

(B) Confirming the reception of the CCC Cleaner (Bot Countermeasure System Operations Group)

The Bot Countermeasure System Operations Group receives the CCC Cleaner updated by the Bot Program Analysis Group, and confirms its operations including whether it can remove the bot and whether it operates properly.

(C) Uploading the CCC Cleaner to the countermeasures web site (Bot Countermeasure System Operations Group)

The Bot Countermeasure System Operations Group uploads the latest version of the CCC Cleaner to the countermeasure site so that the users of infected PCs can download it, enters information reflecting the corresponding sample, and starts the warning process.

③ Requesting the identification of the user of the bot-infected PC (Bot Countermeasure System Operations Group)

Based on the attacker's IP address of the attack event, the Bot Countermeasure System Operations Group identifies the ISP. The group then creates a user identification requesting list to identify the user of the bot-infected PCs, and hands over the list to the ISP and asks them to identity the user.

④ Identifying the user of the bot-infected PC (ISP)

The ISP identifies the user of the bot-infected PC using the attack event data (attacker's IP address and time stamp of infection attack) obtained from the warning system. They also create an identification list that includes the user name, e-mail address, and whether the user is corporate, private, or an ISP.

⑤ Registering the result of identification (ISP)

Using the warning system, the ISP enters the data created in the previous step, assigns a U_ID for uniquely identifying the user in the warning system and the Progress Management System. They then delete (filter) personal information from the identification list and register the contents of the list in the Progress Management System.

⑥ Registering the tracking ID (Bot Countermeasure System Operations Group)

The Progress Management System adds the tracking ID by registering the identification list

and registers the result in the database.

⑦ Issuing a warning to the user (ISP)

The Progress Management System manages the progress according to the scenario conditions set by each ISP and supported by the CCC Cleaner, and generates a warning request list. The ISP obtains the warning request list from the Progress Management System through the warning system. Then they use the warning template that corresponds to the status of the scenario to create a warning e-mail, and send it to the user of the bot-infected PC. (In some cases, the warning is sent by regular mail.)

The user of the bot-infected PC receives the warning e-mail that describes that his or her PC is infected with a bot and the countermeasures that should be taken, with the URL of the countermeasures web site (with a tracking ID).

⑧ Connecting to the countermeasures web site and perform countermeasures (User of the bot-infected PC)

After receiving the warning e-mail, the user of the infected PC accesses the URL (with a tracking ID) listed on the e-mail and removes the bot following the instructions provided.

⑨ Sending completion message (user of the bot-infected PC)

After removing the bot following the instruction on the countermeasures Web site, the user of the infected PC sends a completion message to the Progress Management System indicating that the bot has been removed, by clicking the completion button on the Web site. On receiving the completion message, the Progress Management System ends the scenario and closes the warning.

3.2.2. Increasing efficiency by building systems

(1) Honeypot system

A honeypot system collects malware including bots and attacker's information. When a PC is infected with a bot, it launches infection attacks on neighboring IP addresses. When the infection attack succeeds, the bot controls the PCs to expand the infections.

When we started this project, we adopted malware collection honeypots because the nearer the system is to the environment of PC users, the more positively it can detect bots and the users of bot-infected PCs. In general, honeypots tend to collect files other than malware. The honeypots of this project have a white list function, which prevents the system from processing listed files and directories as malware. Since the collection includes few irrelevant items, the analysis load is alleviated.

The capacity of a honeypot to collect malware and information on attackers largely depends on its design. There are various design techniques for maximizing this capacity.

① Preventing the spreading of infection from one honeypot to another

When a bot infects a honeypot, it attacks the vulnerability of other honeypots through the network. In a malware collection honeypot system, mutual infection could degrade performance. To prevent this, each honeypot is placed in a different network segment and the communication between honeypots is inhibited using firewalls, etc.

② Efficiently detecting bot-infected PCs in Japan

A bot has the characteristic of spreading infection to IP addresses close to the IP address of the infected PC. To effectively detect bot-infected PCs in Japan, we used this characteristic and connected the honeypots to consumer ADSL and optical lines, which are near the IP addresses of infected PCs, from major ISPs.

In addition, for the purpose of assigning a broader range of IP addresses to the honeypot system, we developed a special router that makes use of the characteristic of dynamic IP address lines, and repeats disconnection and connection at regular intervals.

(2) Malware Management Database

The Malware Management Database stores and maintains the infection attack events collected by the honeypot system. This system compares the hash of malware collected by honeypots with existing malware in the database and only registers new malware.

The new malware is sent to the Bot Program Analysis Group where disinfection tools are created.

When the Bot Countermeasure System Operations Group receives a disinfection tool from the Bot Program Analysis Group, they confirm its operation and upload it to the countermeasures Web site so that it is available to the users of infected PCs.

(3) Warning System and Progress Management System

The cooperation of ISPs is indispensable for issuing warnings to the users of PCs infected with bots. For this reason, the overall system has been designed with a concept of alleviating the load of ISPs who send warning messages.

- The systems must be able to keep track of whether warned users have accessed the countermeasures web site and up to which step they have completed.
- Each warning e-mail must be able to be sent in a short time (template e-mail sending).
- The system must allow for fine-tuning, such as adjusting the warning intervals and selecting the text according to the number of resends.
- The countermeasure site that explains the disinfection procedure must be easy to understand and the procedure must be able to be performed by users, which prevents the ISPs from being flooded with inquiries.
- The users' personal information is kept by the ISPs and must not be stored on any servers controlled by the CCC.

The Warning System and the Progress Management System have the following features.

① Progress management using tracking IDs

Managing the progress of users taking countermeasures is essential to the warning workflow. This is implemented with tracking IDs. The implementation method and the procedure for appending a tracking ID are shown in Figure 3-3.

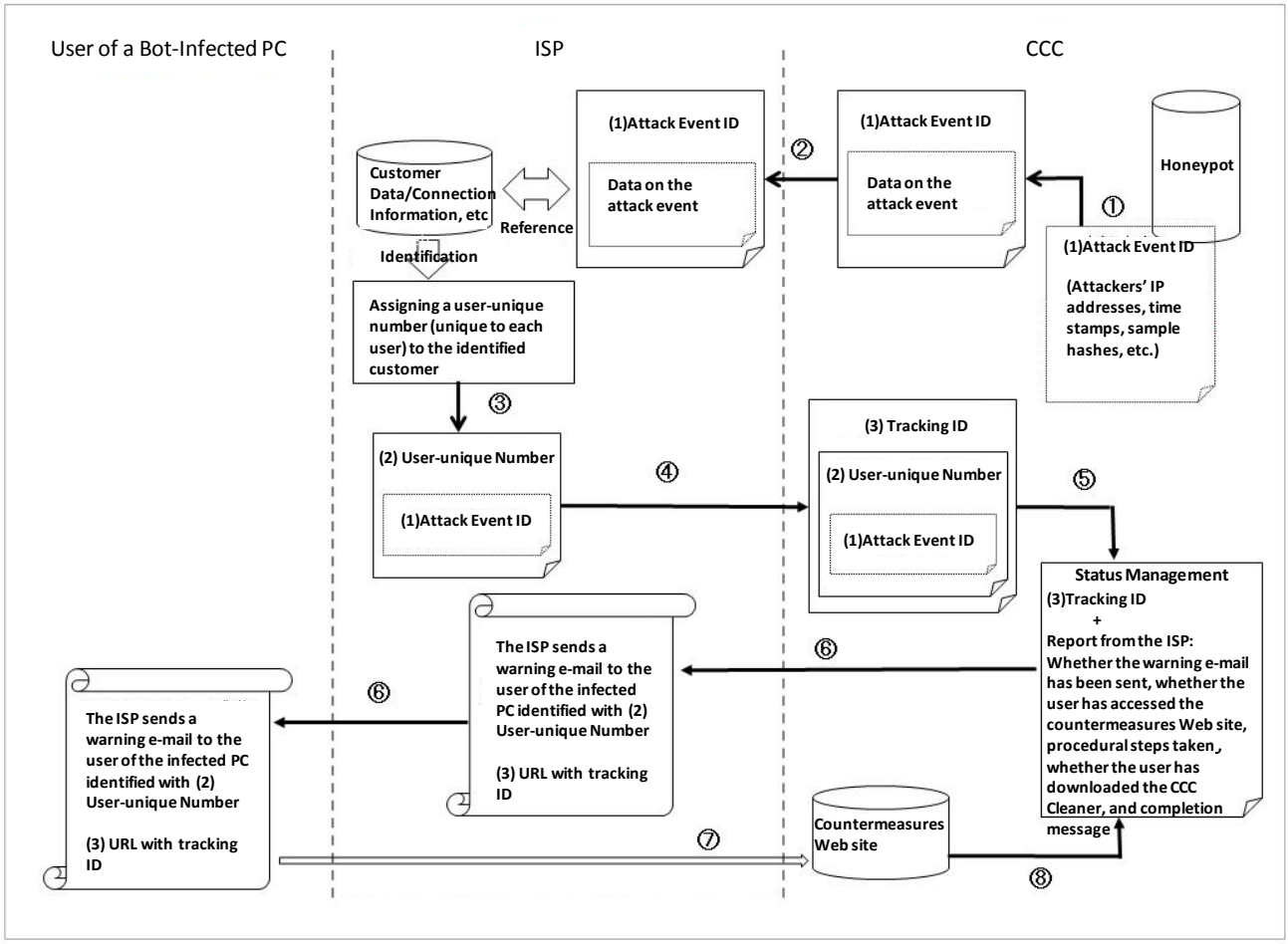


Figure 3-3: Procedure for appending a tracking ID

i. Procedure for appending a tracking ID

The CCC collects the data on an attack event (source IP address, date and time of sending, sample hash, etc.) using honeypots and appends the data with an attack event ID ((1) in Figure 3-3). Then the data is sent to the appropriate ISP identified with the attacker's IP address ((2) in Figure 3-3). The ISP matches the data with its customer and connection data to identify the customer with the infected PC. The ISP cannot easily expose information on the identified user because of the protection of personal/customer information and the confidentiality of communications. Instead they assign a user-unique number and send it to the CCC ((3) in Figure 3-3). The CCC appends this number a tracking ID ((4) in Figure 3-3). Using the tracking ID, the CCC keeps track of the disinfection procedure for this attack event

(sending of warning e-mails, accessing to the countermeasures Web site, performing disinfection procedure, downloading the CCC Cleaner, and sending a completion message) ((5) in Figure 3-3). The CCC also assigns a tracking ID to the ISP and asks them to send warning e-mails. Based on the tracking ID and the corresponding user-unique number, the ISP sends a warning e-mail to the user of the bot-infected PC ((6) in Figure 3-3). On receiving the warning e-mail, the user accesses the countermeasures Web site using the URL with the tracking ID appended indicated in the mail ((7) in Figure 3-3). The user's behavior in the countermeasures web site and the progress in taking countermeasures are monitored using the tracking ID as a key ((8) in Figure 3-3).

ii. Status management using the tracking ID

Some users may not access the countermeasures web site even if their PCs are concurrently infected with several bots or re-infected, or after receiving several warning e-mails. Some users quit in the middle of the disinfection procedure, or there may other reasons they do not complete disinfection. These can be monitored by analyzing the record using the tracking ID. When an attack event occurs, the CCC assigns “A” to the attack event. The ISP assigns a user-unique number “B” to “A.” Then the CCC appends a tracking ID “C” to “B.” When there is another attack event “A2” on the same user, the user-unique number “B” is assigned again. Then the sample data (e.g. hashes) on the attack events “A” and “A2” are compared, and if they are different, it is determined that the PC was concurrently infected with two bots. After a user “B” has sent a completion message, if another attack event “A3” is captured and when the ISP has assigned “B” to the user, it is determined that the PC of the user was re-infected. The CCC keeps track of the progress until it receives a completion message using the user-unique number.

Since the CCC requests the ISP to send a warning e-mail based on the tracking ID, it is clear how many emails have been sent for the attack event ID. The ISP can change the text according to the number of resends (e.g. raise urgency). To save on labor for staged sending, the CCC provides a mail sending tool (Warning Client) to ISPs. Using this tool, the ISPs can define several texts with staged urgency levels, and using the send list with status (e.g. number of resends) from the CCC, automatically select an appropriate message and compose an e-mail.

② Opening the countermeasures web site

Conventional warnings to the users of virus-infected PCs given by ISPs have been in the form of e-mails that explain how to disinfect their PCs. However, this method is not so effective because some users do not understand the contents, and do not try or are unable to take the necessary measures. These results in a low completion rate, raising the urgency level, and this can become a vicious circle. To prevent such a situation, we have set up a web site that explains the procedure for disinfection and the measures for preventing re-infection in plain

language so that warned users can undertake countermeasures themselves. In addition, since each user accesses this web site using the URL appended with a tracking ID, the CCC can keep track of the procedural steps taken and confirm the completion. The data obtained is stored in the Progress Management System, which maintains the warning status. Sharing the status of infection and measures taken on each user between ISPs and the CCC is effective for user support and revising warning activities.

(4) Public web site

In addition to the countermeasures web site that is accessed through ISPs, we have a public web site for general anti-bot measures (https://www.ccc.go.jp/) (Figure 3-4). This web site aims to raise awareness of the “threat of bots” by providing necessary information to users in general. Everyone can access this Web site, have his or her PC checked for bot infection, and remove them if infected. The web site describes how to build a bot-free and safe PC environment. As it is impossible to detect all PCs infected with bots, this site serves as a place to educate the public by announcing its existence through mass media. etc.

Figure 3-4: Public Web Site

3.2.3. Problems and solutions in the project

Operating the Warning System and Progress Management System completes the process of collecting bots, detecting bot-infected PCs, and warning the users about infected PCs. As estimated, we could collect a large number of bots and detect bot-infected PCs during the early period of our activities. However, in 2009, the number of collected bots and the number of detected infected PCs

started to decrease. This could be not just because our activities reduced the number of infected PCs, but the result of attackers taking countermeasures against the honeypot system. To cope with this, we developed a new honeypot system. We also continue our efforts to improve the efficiency of the warning procedure.

The countermeasures against the decline in the number of warned users and the efforts on raising awareness of the countermeasures web site as a part of increasing the efficiency of warning activities are described as follows.

(1) Countermeasures against the decline in the number of warned users

① Introduction of Attack Event Detection Honeypots

Following the design policy of "being able to inform the users of bot infection with certainty," malware collection honeypots target only the IP addresses in which bots could be collected from the attacker. If there is an infection attack but the bot cannot be collected, or if the collected bot does not work, no warning is generated.

Since October 2008, the number of warned users started to decline and the gap between the actual infection rate and the number of collections widened. Thanks to the log reporting function added to the CCC Cleaner in November 2007 (see (4)-(1) "Collecting CCC Cleaner logs"), it is now possible to analyze the status of infected PCs. The analysis revealed thatusers' PCs were infected not only with the bots captured by the CCC but a variety of other malware and unknown viruses. Having considered this fact, we thought the initial concept of "warning only the user with the IP from which the bot could be captured" is not sufficient, and it was necessary to warn also the users of the PCs that launched infection attacks where the bot had not been captured. In this case, it is necessary to distinguish only the attacks that should be warned by precluding events such as port scanning where there is no infection attack. In June 2009, we introduced attack event detection honeypots, the low-interaction type that can discriminate between patterns of vulnerability attacks. Combining two types of honeypots, both efficient warnings to users of infected PCs and the collection of various bots have been realized.

(2) Efforts on increasing the rate of visiting the countermeasure web site

① Optimizing e-mail resend interval

The Warning System allows the resend interval and the number of re-warnings to be adjusted by setting up a scenario. The analysis of results revealed that the rate of visiting differs according to the resend interval. In the case of an ISP that sent a total of three e-mails once a week, the visiting rate fell short of 20%.

According to surveys, an e-mail newsletter is read most in the first three days from the date of sending, and rarely read after that. Therefore, even if an e-mail is sent to a user who has not accessed the countermeasures web site one week after sending, mail may not be read on that day of the week, or it is read but no countermeasure is taken because the user is busy, etc.

When the resend interval was changed to three days (sent every three days), the reading rate remained the same. However, the shift in the reception day of the week promoted taking countermeasures, which resulted in a 10% increase in the visiting rate.

② Modifying the e-mail text

Even after three days, warning e-mails could be left unread. According to a survey, e-mails with【重要】(Japanese for “Important”) in the Subject are not recognized as such because that title is often used in spam mail. We changed the subject to【緊急】(Japanese for “Urgent”), which is not used so often, and indented the word by one character space so that it stood out in the subject list.

People tend to judge the importance of an e-mail by scanning the first several lines rather than reading the entire text. Those lines were changed to warn that the user’s PC is at a risk. We also introduced techniques used in mail magazines to increase the rate of visiting the countermeasures web site. These included surrounding the important sentence with ruled lines and placing the main topic at the top and making it more concise.

③ Warning by regular mail

Warning e-mails are mainly sent to the e-mail address of the ISP. However, since more and more people use web mail, such as Yahoo! Mail and Gmail, warning e-mails sent to the ISP’s mail account could not be read. Even if a user receives a warning e-mail from the ISP, he or she may not aware of its importance.

Some ISPs started giving warnings by postal mail, but the rise in costs became a major problem. However, with e-mail warnings, the visiting rate was as low as 30%. Assuming that sending postal mail is more effective than sending dozens of unread e-mails, we decided to send a postal mail if the user has not visited the countermeasures Web site after receiving two warning e-mails.

This method has raised the visiting rate from 30% to 60% but it is still lower than our expectation. We interviewed target users using outbound calls, and found that they thought the mail was direct mail because it was in the same type of envelope used for direct mailing from the ISP.

We asked the ISP to use an envelope with a different design from direct mails, to avoid using a “Confidential” or “Important” mark that is often used in direct mails, and print a message in red indicating that it was a warning about line usage, with the expectation that the recipients recognized the importance of the mail. These measures have increased the visiting rate to 80% or higher, and decreased the number of warned users.

④ Telephone support by ISPs

Most call centers of ISPs in Japan provide toll-free services. On the other hand, for telephone support by PC manufacturers, OS developers, and anti-virus software companies,

the users pay for the call and sometimes also for inquiries. This encourages users to call ISPs. However, most ISPs do not provide support on malware infection, and when they receive such inquiries, they recommend the customer to call the PC manufacturer, OS developer, or anti-virus software company, where the customer does not receive adequate support but is often advised to initialize the PC

Even if the PC is initialized, it is often re-infected because few manufacturers give advice on network-type infections.

In order that users receive proper support, the CCC is holding seminars for ISPs, in which we describe what happens when a PC is infected and the importance of the router when the PC is initialized.

Some users ask PC manufacturers for support but give up because they cannot describe exactly what is happening, the call center is busy, or do not know what to do to recover. According to analysis of progress records, there are users who tried to disinfect their PC but somehow quit in midstream and then did nothing further.

These users do not (or cannot) take measures no matter how many times they receive warnings in the conventional way. Some ISPs receive inquiries on security measures inbound although they are not included in the scope of their support.

Apart from the procedure for initializing PCs, carried out by PC manufacturers, those ISPs provide one-stop remote support up to the recovery and prevention of re-infection, which results in high recovery rates.

(3) Optimizing the countermeasures procedure

The procedure described on the countermeasures Web site consists of the following steps:

1. Running Windows Update.
2. Executing the CCC Cleaner.
3. Installing anti-virus software.
4. Installing a router.

Earlier, step 1 and step 2 were reversed because Windows Update takes a long time and we thought it was better to disinfect with the CCC Cleaner first. However, in such a procedure, the bot was removed but the root cause of the infection attacks were not fixed, and there were many cases in which PCs were infected before Windows Update was run. This is why we altered the procedure. A router should be installed after the external infection attacks are stopped but the user has to purchase it, which interrupts the procedure. As it was expected that users would skip this step because they have not purchased a router, the step remains as it is.

(4) Other techniques and improvements

① Collecting CCC Cleaner logs

The CCC Cleaner has a function for creating a log[5] of the result of disinfection. We have added the feature for sending the log to the CCC, which is helpful for analysis.

Sending the log requires the consent of the user. The user can allow or reject sending.

② Handling of the WORM_DOWNAD virus by the CCC Cleaner[6]

As the CCC Cleaner is executed under PC Administrator authority, it cannot remove WORM_DOWNAD that runs under the SYSTEM authority. Some anti-virus software companies provide a dedicated tool for removing WORM_DOWNAD. However, as accessing the domains of anti-virus software companies from a WORM_DOWNAD-infected PC is restricted, it is difficult to obtain the tool and disinfect. In such a case, the only solution is to initialize the PC, which is a great obstacle to disinfection, and in some cases the PC is left without taking any measures. To cope with this, the CCC made the "WORM_DOWNAD removal tool," developed by Trend Micro Incorporated, available on the CCC domain server. Users can obtain the tool without being affected by the domain restriction.

③ Telephone support by the CCC

At the beginning, the CCC only answered inquiries by e-mail. However, with e-mails it is difficult to know in which step the user is having trouble, what the user has in mind, etc. Therefore, to improve the procedure and create comprehensive help, it is necessary to understand the status of the user. For these reasons, we are asking users to include their telephone numbers in their inquiries. We provide user support by calling them back and considering their reactions to the procedure.

In contrast to obtaining information through ISPs, talking directly with users and listening to the details of what is happening are very effective in understanding countermeasure effectiveness.

④ ISP seminars and lectures

To approach more users of bot-infected PCs, it is necessary to solicit the participation of more ISPs to the project. Since 2008, we have held ISP seminars twice a year. The initial purpose was to increase the number of ISP participating in the project. Now, in addition to calling for participation, we introduce the latest trends of bots and examples of successful anti-bot measures, and share information, with the intention that the ISPs can perform warning

---

[5]The Disinfection Log records the operating system, Service Pack version, IP address type (global or local), memory capacity of the PC, names of malware removed, number of items removed, and the number of failures.

[6] WORM_DOWNAD is a worm-type virus that uses vulnerability MS08-067 for which Microsoft Corporation issued an urgent release of patch in October 2008. In addition to the vulnerability, subspecies infect through USB memory sticks, removable media, and Web sites. Infections from this virus have been increasing in Japan

activities and promote countermeasures more effectively. In 2009, we also hosted a lecture for ISPs' customer support staff.

3.3. Achievements

The monthly and cumulative totals for warning activities by the CCC since May 2007 are shown in the public Web site (https://www.ccc.go.jp).

3.3.1. Achievement of warning activities in March 2010

The total cumulative number of malware samples including bots collected by the honeypot system is 16 million (the number of malware types is one million). Of these, approximately 30,000 unknown malware samples have been obtained. The warning activities by participating ISPs have sent the cumulative total of approximately 480,000 warning e-mails to approximately 100,000 users.

31.6% of the warned users have downloaded the CCC Cleaners and taken countermeasures. On the public web site, the CCC Cleaner has been downloaded more than 1,2 million times (cumulative).

The accomplishment of warning activities published in March 2010 is shown in Figure 3-5.

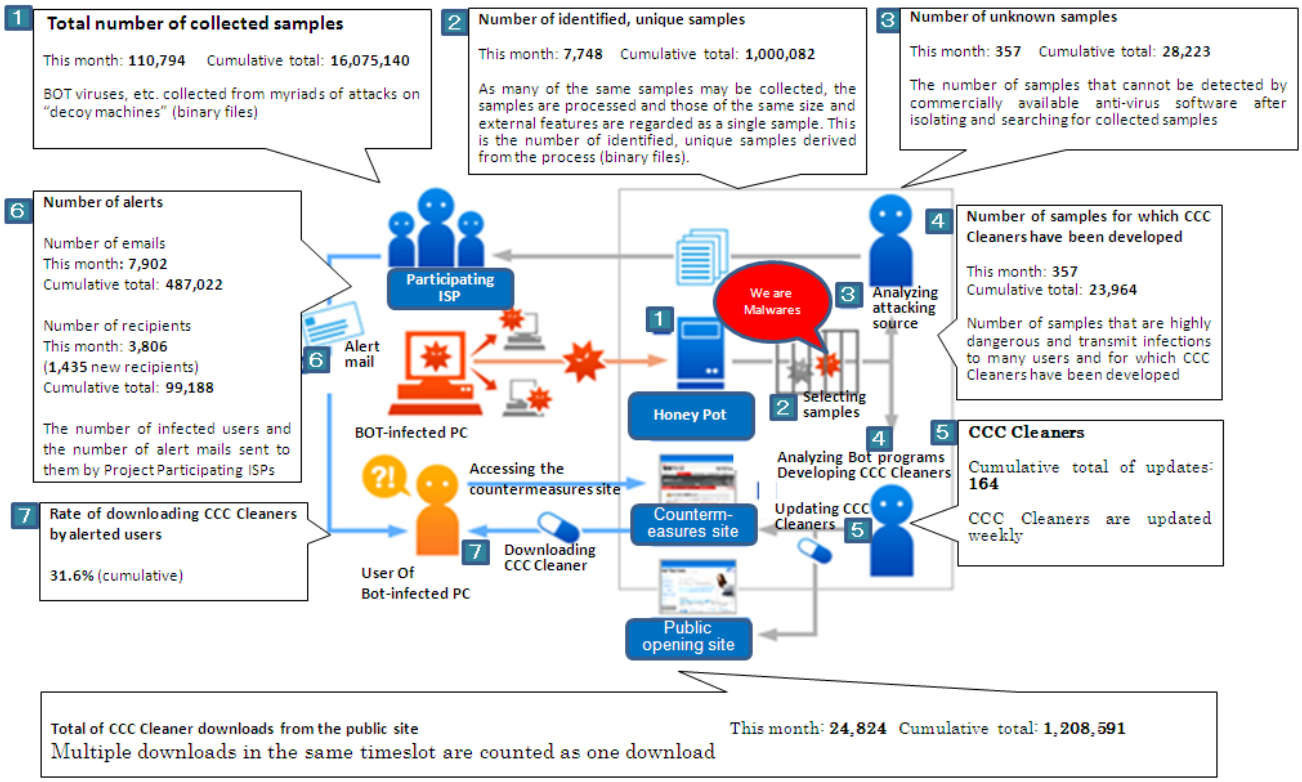


Figure 3-5: Achievement of warning activities in March 2010

3.3.2. Trend in the number of malware samples collected

The total number of malware samples collected is shown in Figure 3-6. The horizontal axis indicates the time (in days) and the vertical axis the number of samples. The blue bars show the number of existing malware samples that could be detected by anti-virus software. The red bars show the number

of unknown malware samples that could not be detected.

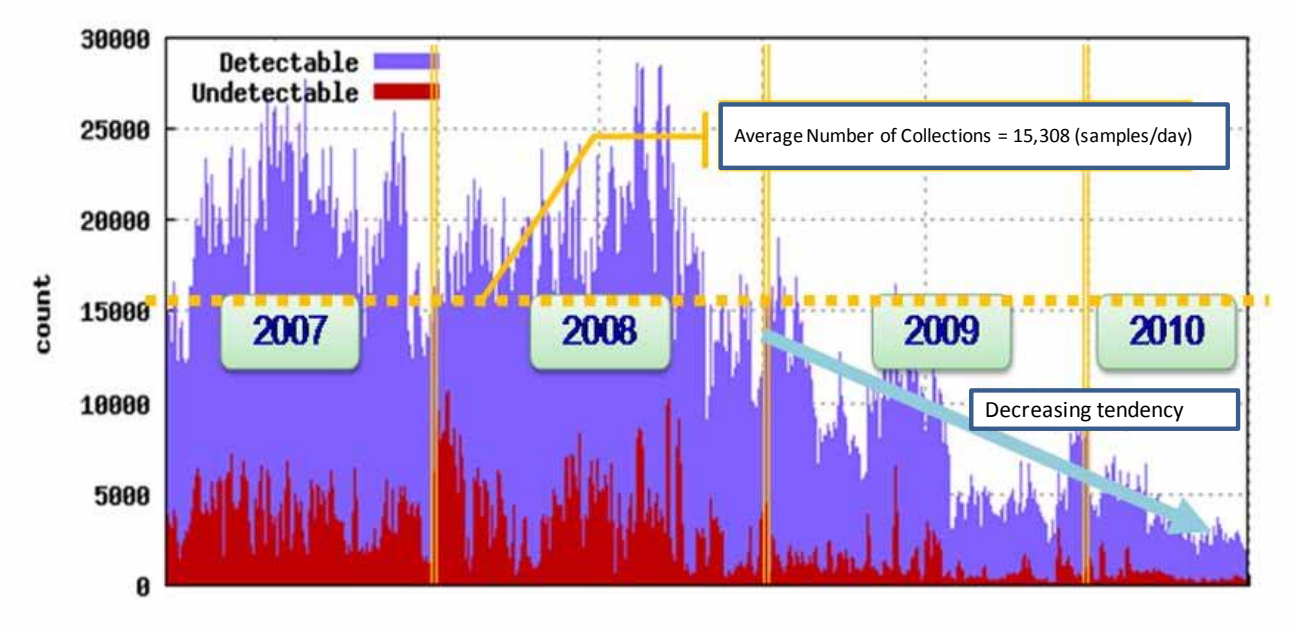


Figure 3-6: Trend in the total number of malware samples detected

The ratio of unknown malware samples to the total number of malware samples collected (Undetectable / (Detectable + Undetectable)) is 16% on average. The number of samples collected has started to decline since 2009. In fiscal year 2010, the decline is more noticeable.

Looking closely at each year, in 2007 and 2008, more than 5 million samples (both known and unknown) were collected. The reason for the known malware was that the PE_BOBAX-type and PE_VIRUT-type file infection viruses, which infects other files within a PC, actively replicated in the honeypots.

For the unknown malware, a large number of new malware was collected every week from a malware distribution Web site in Canada. Since 2009, the number of collections has decreased significantly because the number of file infection viruses declined and the collections from the malware distribution web site in Canada has decreased.

3.3.3. Trend in the number of warnings

The trend in the number of warned users is shown in Figure 3-7. The chart indicates that the newly warned users are in decline, which means that the number of users of bot-infected PCs is also steadily declining.

The number of re-warned users is also decreasing. However, comparing April 2007 and June 2010, the amount of decrease is smaller then the decrease in new users. This may be because the users who do not respond to the first warning tend not to respond to subsequent e-mails.

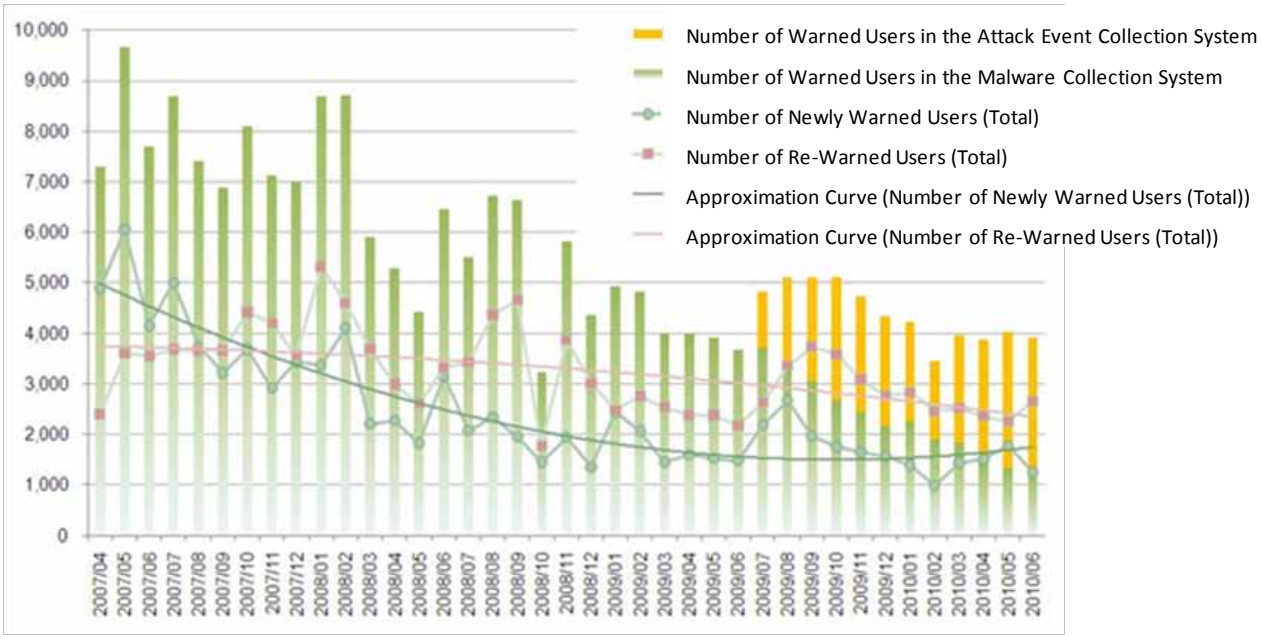


Figure 3-7: Trend in the number of warned users (April 2007 to June 2010)

The response rate on the countermeasures web site (the ratios in percent of the numbers of users who accessed the top page of the countermeasures web site, who accessed the Microsoft Windows Update site from there, who downloaded the CCC Cleaners, and who clicked the Completion Message button to the number of warned user) by fiscal year are shown in Figure 3-8.

In 2007, the ratios of the users who accessed the Microsoft Windows Update Web site and who downloaded the CCC Cleaner were 22% and 30%, respectively. In 2008, they reversed, and were 43% and 29%, respectively. This was because the disinfection procedure steps ware altered in 2008 and running Windows Update came before downloading the CCC Cleaner.

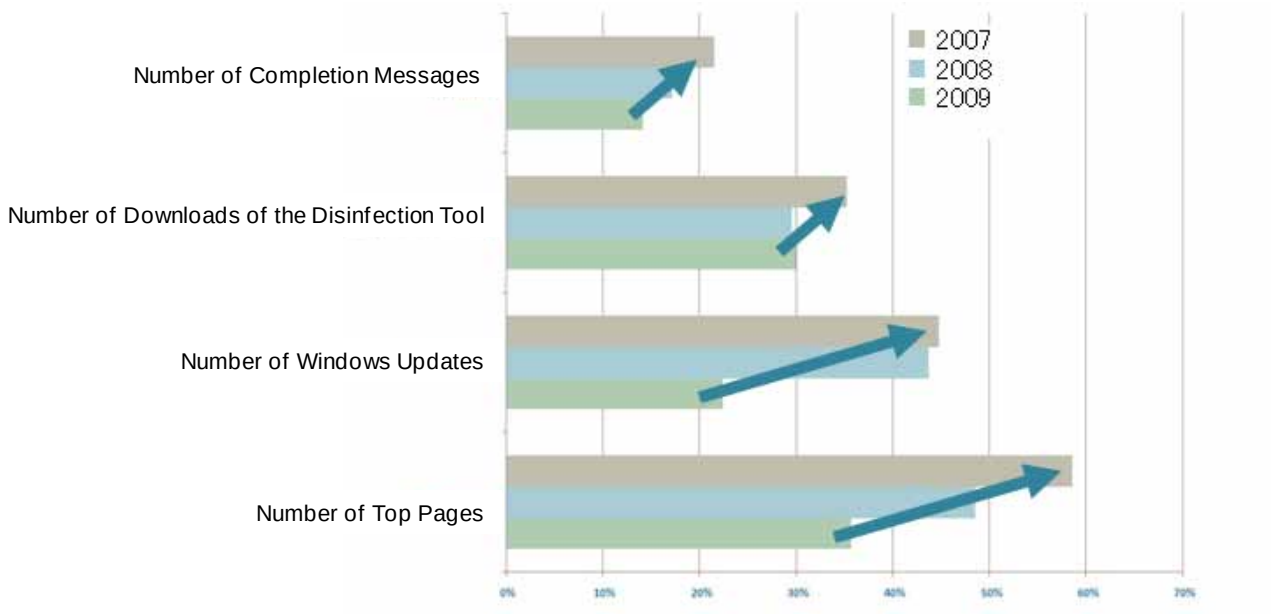


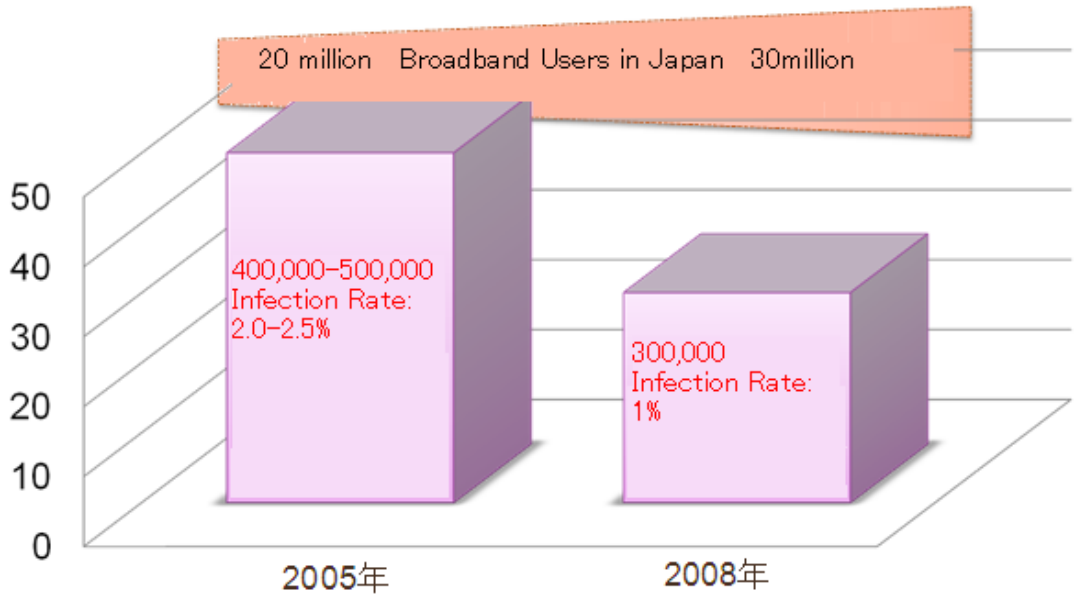
Figure 3-8: Rate of warned users taking countermeasures

3.3.4. Trend in infections

According to a survey conducted by Telecom-ISAC Japan and JPCERT/CC in June 2005, before the project started, the PCs of 400–500,000 users out of the total 20 million[7] broadband users in Japan were infected with bots (infection rate was 2.0–2.5%).

The CCC started its anti-bot activities in 2006. In June 2008, a similar survey performed by the CCC estimated that the PCs of 300,000 users out of the total 30 million[8] broadband users were infected (infection rate was approximately 1%).

The trend in the number of the broadband users of bot-infected PCs and the infection rate in Japan are shown in Figure 3-9.



Source: Telecom-ISAC and JPCERT/CC

Figure 3-9: Number of the broadband users with bot-infected PCs and infection rate in Japan

Although the number of broadband users has increased by 10 million in three years, the infection rate has declined, which indicates the project yielded practical results. However, this is not only the result of our efforts but because the operating systems on the PC have themselves become more secure, which has reduced the risk of infection by simply connecting to the Internet.

[7] Estimated from MIC statistics “Trend in Broadband Service Subscribers”

4. Activities of the Bot Program Analysis Group

4.1. Activities

The Bot Program Analysis Group analyzes the bot samples collected with honeypots operated by the Bot Countermeasure System Operations Group, and creates disinfection tools to remove the bots from infected PCs as described in 3.1. The major activities of the three CCC groups are shown in Figure 4-1.

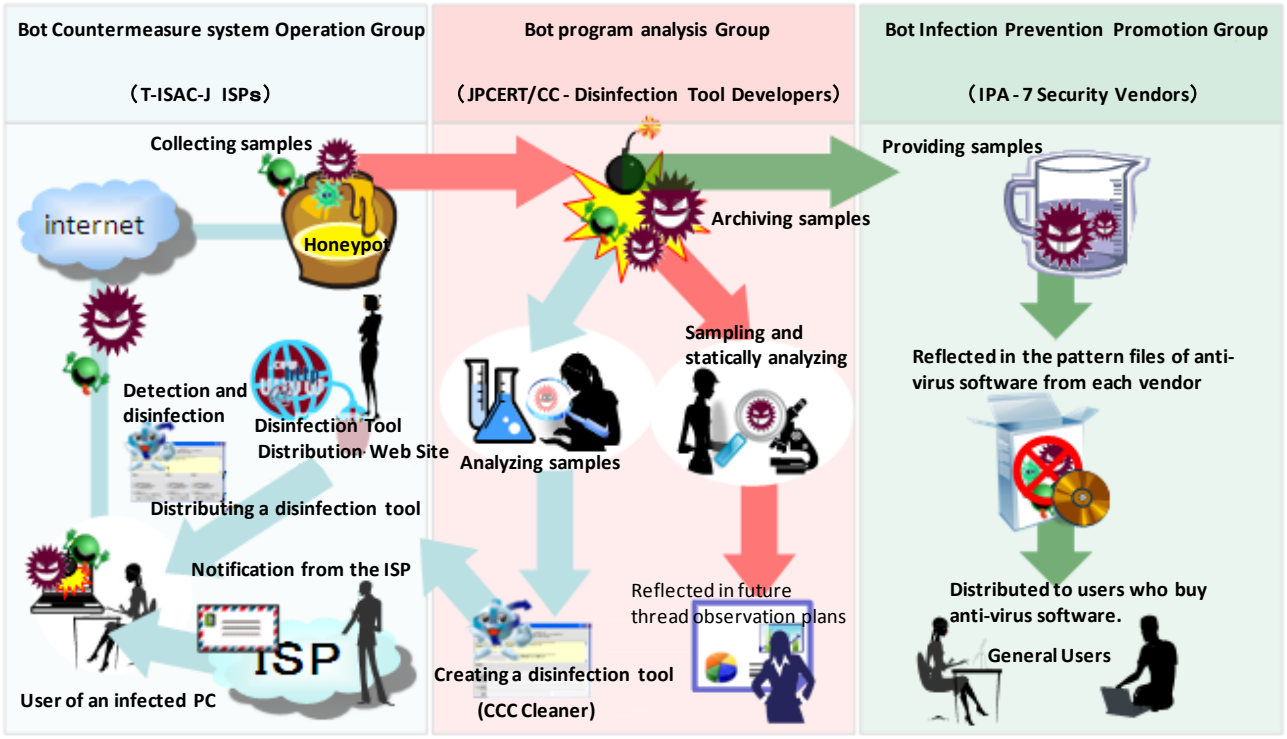


Figure 4-1: Roles of CCC groups

1. Distribution of a disinfection tool (CCC Cleaner)

The Bot Program Analysis Group analyzes the samples collected with the honeypots operated by the Bot Countermeasure System Operations Group, and creates a disinfection tool (CCC Cleaner) from the results of the analysis and distributes it.

2. Detailed analysis of collected samples

The group analyzes distinctive samples collected with honeypots in detail and reflects the results against future vulnerability predictions and in the measures to be taken. They also investigate the logs sent by the information transmission function implemented on the CCC Cleaner in fiscal year 2008.

3. Providing samples to the Bot Infection Prevention Promotion Group

The group also provides the Bot Infection Prevention Promotion Group with collected samples so that the samples are reflected in the creation of pattern files for anti-virus software.

This report focuses on the activities undertaken in fiscal year 2009, specifically the creation of the CCC Cleaner, and the analysis of the logs and samples.

The center of activities of the Bot Program Analysis Group is the analysis of the malware (hereafter, “samples”) collected with the honeypots operated by the Bot Countermeasure System Operations Group. This section mainly describes the creation of the CCC Cleaner, and the analysis of the logs and samples.

4.2. Creation of the CCC Cleaner

The Bot Program Analysis Group analyzes the samples that are not supported by anti-virus software in the market and reflects the results in the development of the CCC Cleaner, which is a simple disinfection tool.

In fiscal year 2009, the group reviewed its operations to increase the efficiency of the development of the CCC Cleaner so that the tool can be supplied reliably. To be more specific, they automated some manual tasks, and divided the work of checking the operation of the tool among several people. The CCC Cleaner has been updated 164 times. The following list shows how the samples collected by the honeypots have been reflected in the revision of the CCC Cleaner since February 2007. The cumulative rate of reflection is 99.47%.

1) Number of samples reflected in the CCC Cleaner: 23,964
2) Number of known samples: 970,814
3) Number of identified samples: 1,000,082
4) Rate of reflection in the CCC Cleaner: ((1) + (2)) / (3) = 99.47%

This indicates that 99.47% of the collected samples can be detected by the CCC Cleaner and anti-virus software. It can thus be said that the group is making full use of the collected samples.

1) Number of samples reflected in the CCC Cleaner
   The number of samples that have not been detected with anti-virus software but reflected in the CCC Cleaner.
2) Number of known samples
   The number of samples that have been confirmed to be supported by the CCC Cleaner at the time of the collection.
3) Number of identified samples
   The number of unique samples. (Many occurrences of the same sample are collected.)

Functions of the CCC Cleaner

When revising the CCC Cleaner, the Bot Program Analysis Group reviews its functions, not only disinfection, from the users' viewpoint. The following section describes the functions of the CCC Cleaner.

(1) Notification of file infection bots

When a file infection bot is executed, it infects files in executable form such as application files and system files, one after another. Because of this characteristic, this type of bot is difficult to detect. There is also the possibility that even after disinfection by the CCC Cleaner, the PC remains infected. For this reason, when the CCC Cleaner detects a file infection bot, it issues a popup warning (Figure 4-2).

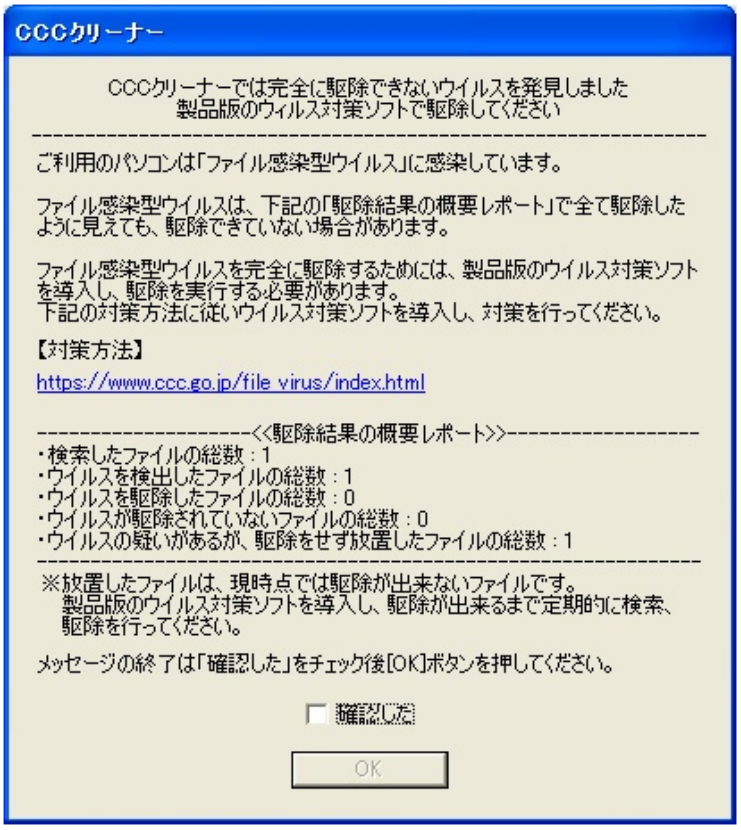


Figure 4-2: Popup warning issued when a file infection bot is detected

If important files under the system folder have been infected and it is impossible to disinfect, the disinfection process is terminated because isolating pertinent files could cause problems, such as disabling the operating system from starting up (Figure 4-3).

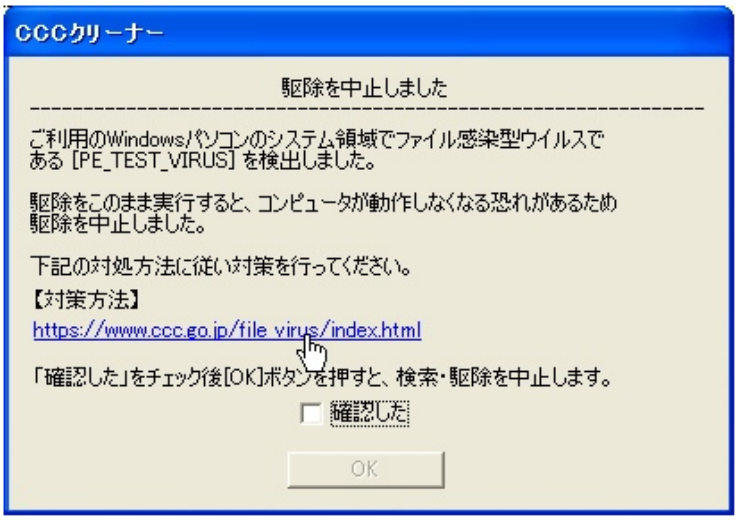


Figure 4-3: Popup warning when disinfection has been terminated

(2) Information transmission function

In order to analyze the state of the PC and the information on its operating environment, and exploit them for planning effective measures, the CCC Cleaner has a function to detect and send such information. The user can allow or reject this transmission. The information sent (transmission log) includes the following items (Table 4-1).

Table 4-1: Information Sent

Item	Description
Execution time	The date and time when the tool was executed, and the time taken to scan the PC
Operating system	The operating system version and the Service Pack (SP) applied
Memory	The amount of physical memory
Networking environment	IP address type (global or private) of the operating environment
Hosts file	Whether the user's hosts file has been tampered with
Result of disinfection	Number of files and error information
Detected malware	The name of detected malware, and the SHA-1 hash of the pertinent file

The analysis of the transmission log, which has been performed this fiscal year, described in 4.3.2.

(3) Host files tamper recovery function

The tool has a function for recovering the host's affected files to prevent these files from hindering update of the Microsoft Windows Update or anti-virus software. If tampering of the hosts file is confirmed, the tool issues a warning (Figure 4-4). When the user selects "Recover," the tool

creates a backup of the hosts file and recovers it to the default state.

Figure 4-4: Popup issued when file tampering has been detected

(4) Service Pack application checking function

Microsoft Windows has an automatic update function. However, some systems may not necessarily have been updated to the latest state because the function could have been disabled by malware or because the user simply does not perform Windows Update. For this reason, the CCC Cleaner detects the latest Service Pack (SP) and security patches applied to the PC, and when it determines the PC is not at the latest level, it issues a popup warning (4-5) to recommend the user to perform Windows Update.

Figure 4-5: Popup warning issued when a necessary update has not been executed

(5) Connection type checking function

A PC connected directly to the Internet is more susceptible to malware infection compared to a PC connected via a broadband router.

For this reason, the CCC Cleaner has a function to check whether the IP address assigned to the PC is a global IP address or private IP address. If a global IP address is assigned, the tool issues a popup warning (4-6) to recommend using a broadband router.

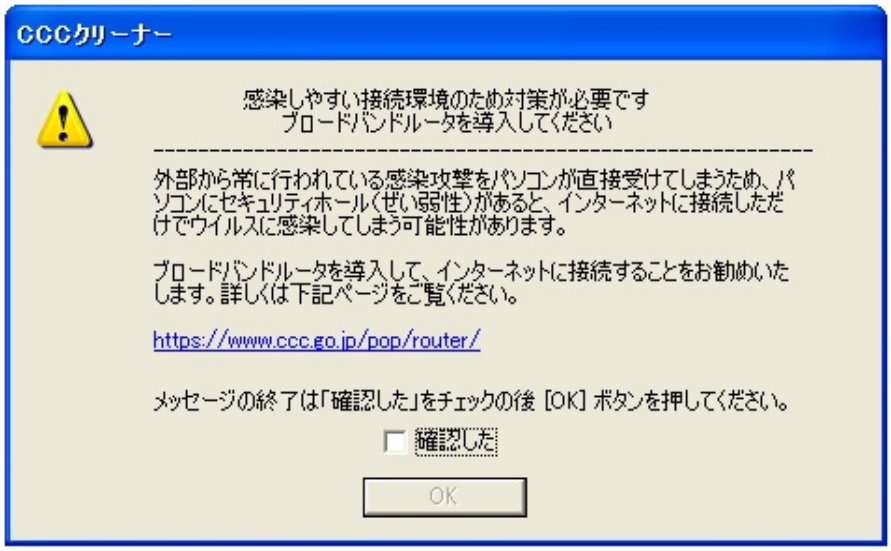


Figure 4-6 : Popup warning issued when a global IP address is assigned

(6) Expiration period

Since the CCC Cleaner does not have a function for automatically updating its pattern file, it has an expiration period so that the tool cannot be used beyond that period. The expiration period encourages users to download the latest revision and run it. When a CCC Cleaner revision expires, it issues a popup warning (4-7).

Figure 4-7: Popup warning issued when a CCC Cleaner revision expires

4.3. Analysis of bots

4.3.1. Outline of bot analysis

(1) Purpose

With the aim of estimating future threats and studying preventive measures, the Bot Program Analysis Group analyzes the bots currently prevalent to identify them, accumulates findings, and examines the data collected.

(2) Target

The group analyzes two types of data: logs sent from CCC Cleaners and samples collected using the honeypots.

① Logs sent from CCC Cleaners

Analyzing the logs sent by CCC Cleaners provides the following information:

- Information on the PC environment in which the CCC Cleaner runs
- Information on malware prevalent
- The difference between the bots detected by the PC on which the CCC Cleaner runs and the samples collected by honeypots

Combining the above information with an analysis of the samples collected by the honeypots leads to planning more effective countermeasures.

② Samples collected by the honeypots

These samples are malware collected by the honeypots operated by the Bot Countermeasure System Operations Group. Detailed analysis of the samples clarifies the behavior of the malware, which enables keeping track of the trends and changes, as well as estimating future threads and planning countermeasures.

The trend of the collection in fiscal year 2009 is shown in Figure 4-8.

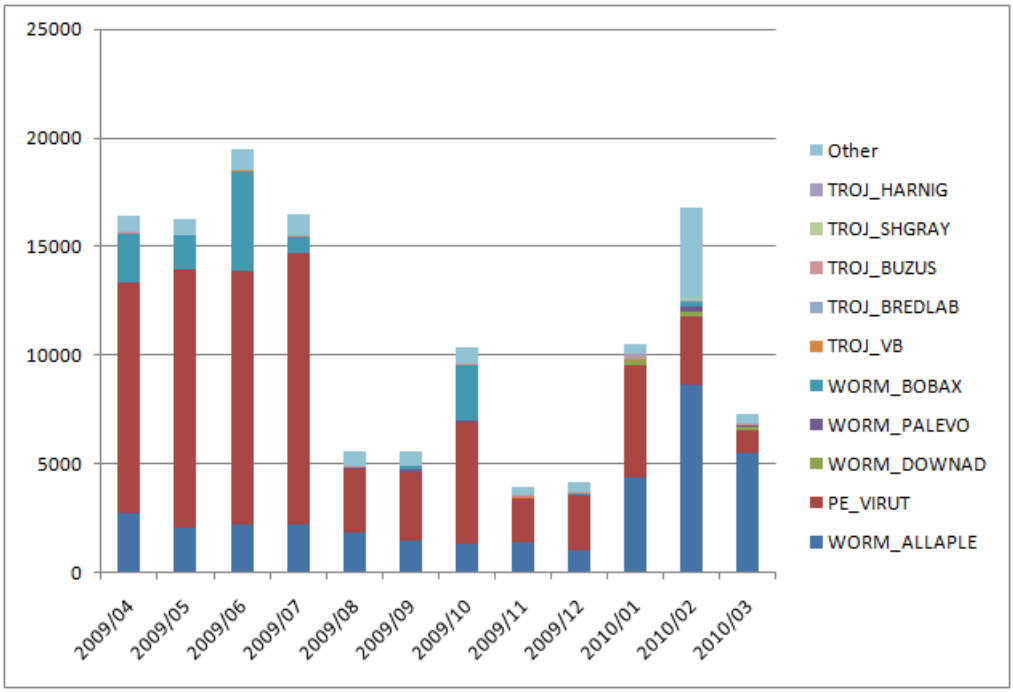


Figure 4-8: Trend in sample collection using honeypots

4.3.2. Analysis of the logs sent from CCC Cleaners

(1) Trends concerning logs

① Number of logs received

The trend in the number of logs received is shown in Figure 4-9. There are increases in April, September, and October 2009. This was because more people downloaded the CCC Cleaner following the media reports on the CCC's activities.

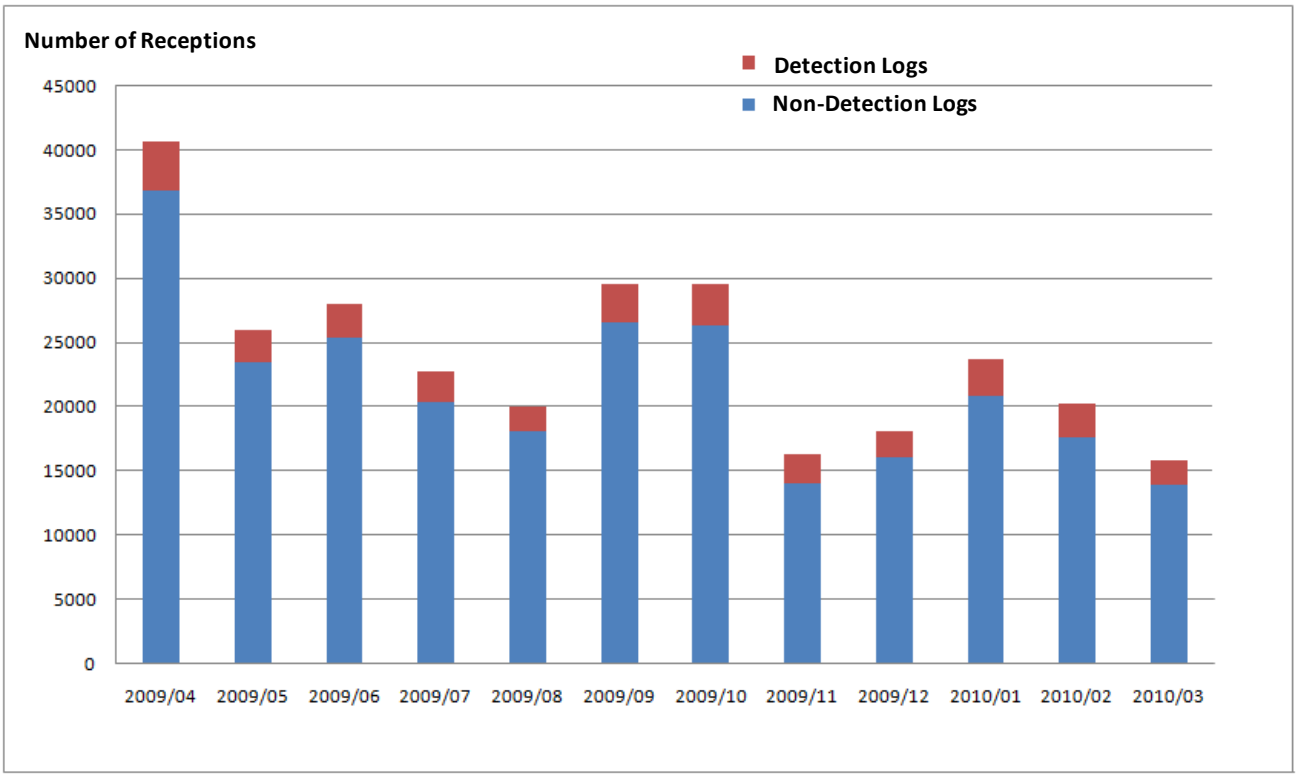


Figure 4-9: Trend in the number of logs received

② Trend in the ratio of Windows operating systems

The trend in the ratio of Windows operating systems and application of Service Packs in the environments in which the CCC Cleaner runs is shown in Figure 4-10. Since January 2009, installation of Windows XP SP3 and Windows Vista SP2 has been increasing. We believe this is because the Service Pack application checking function recommended the users to apply these SPs.

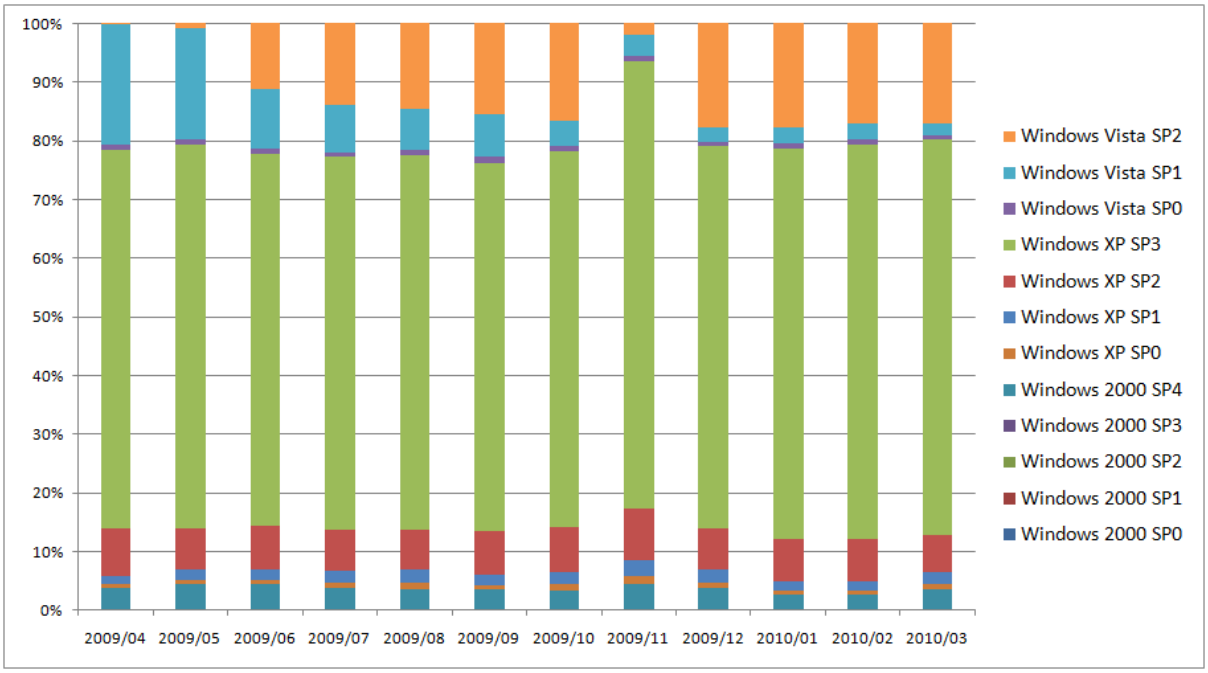


Figure 4-10: Trend in the ratio of operating systems

③ Trend in the detection of malware

The trends in the detection of malware for the users of the Public Web Site and the users notified of bot infection are indicated in Figure 4-11 and Figure 4-12. For the Public Web Site users, samples that try to steal online game accounts (e.g. WORM_ONLINEG) and samples that use the autorun function of removable media (e.g. Mal_Otorun) are prominent. For the notified users, the detection trend is similar to the collection trend illustrated in Figure 4-8 when file infection malware PE_VIRUT was found. Other than PE_VIRUT, similar to Public Web Site users, there are many cases of samples that use the removable media's autorun function. The spread of infections by malware that had not been collected with honeypots was also found.

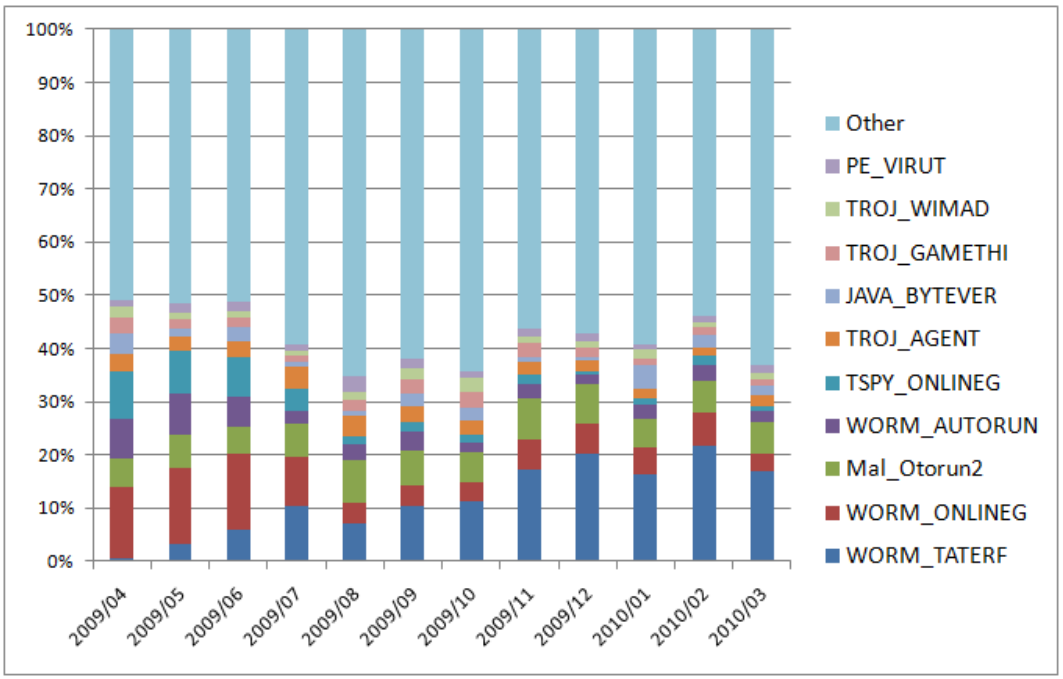


Figure 4-11:Trend in detection for public web site users

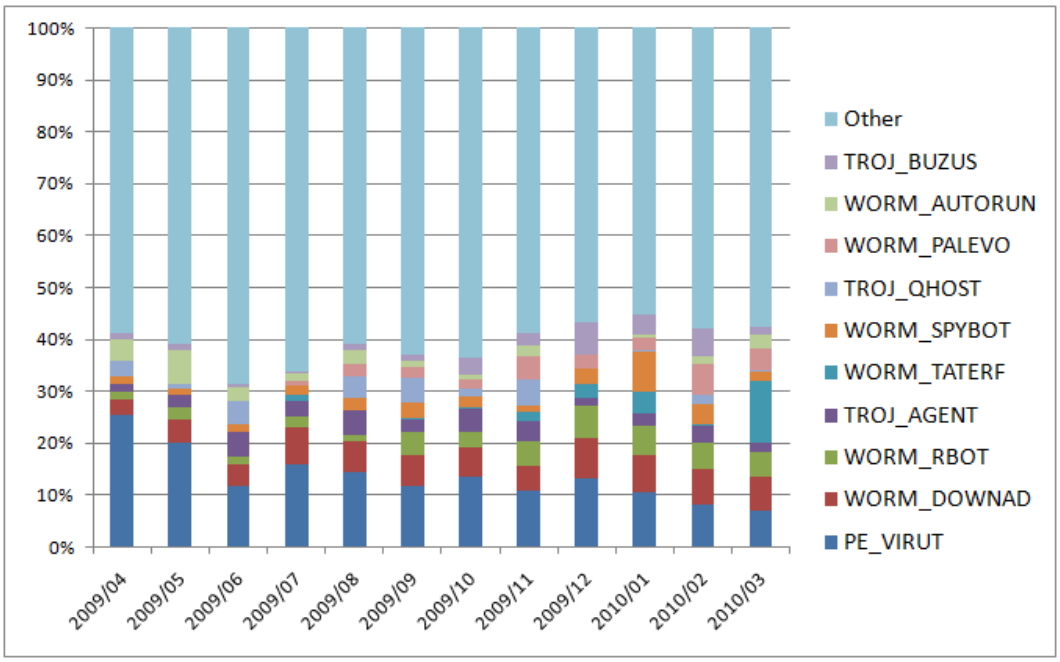


Figure 4-12: Trend in detection for notified users

④ Detection rate by Windows operating system SPs

The detection rate by Windows operating system SPs for Public Web Site users and notified users are shown in Figure 4-13 and Figure 4-14. What is common between the two types of users is that as the SP version rises, the infection rate decreases, and that Windows Vista indicates a low infection rate.

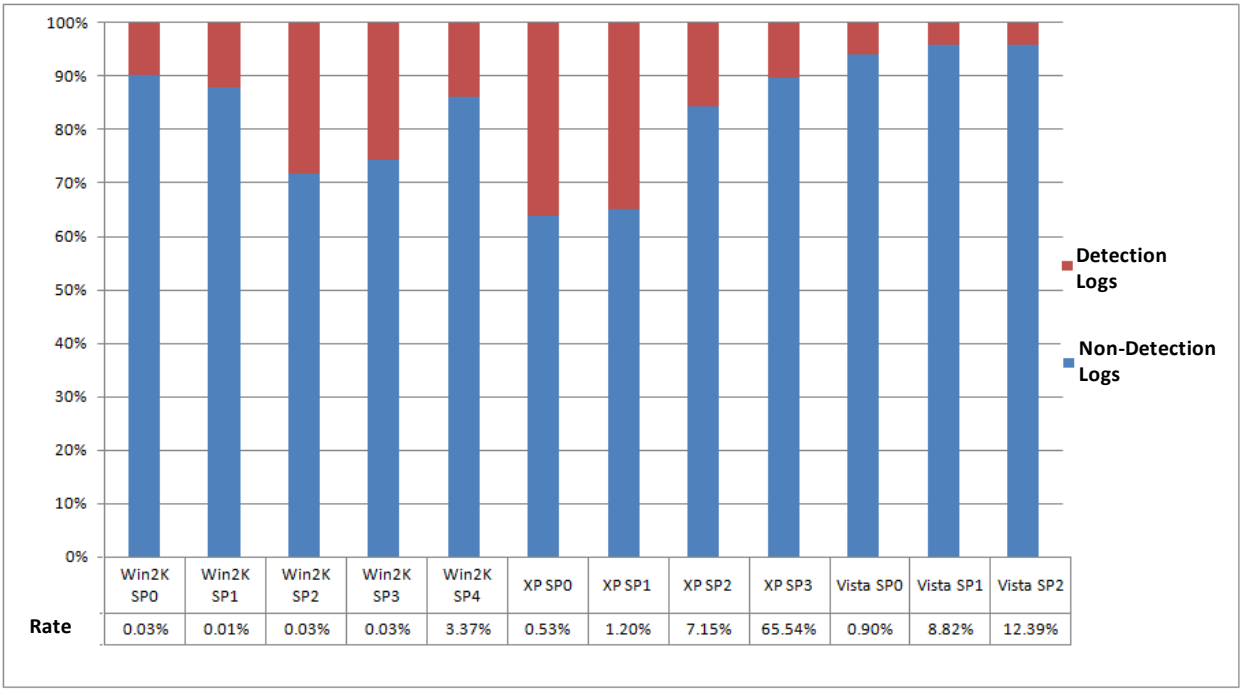


Figure 4-13: Detection rates by Windows OS SP (Public Web Site users)

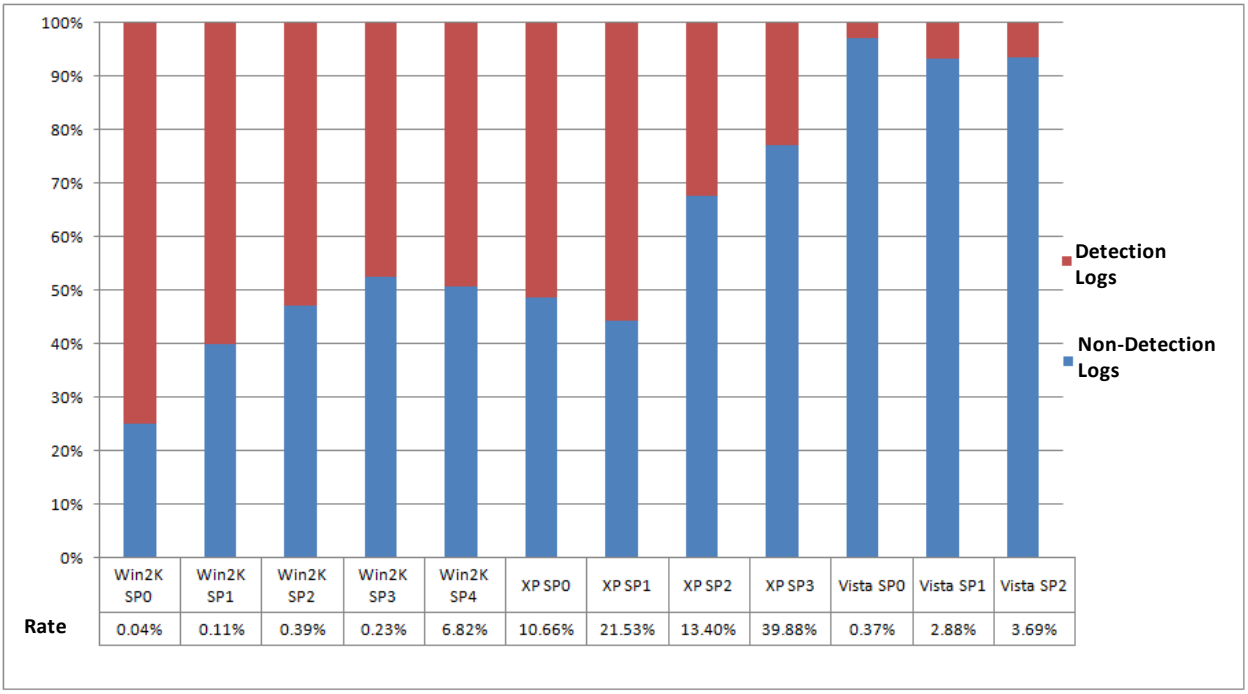


Figure 4-14: Detection rates by Windows OS SP (notified users)

⑤ Trends in networking environment (IP address type)

The IP address types of Public Web Site users and notified users are shown in Figure 4-15 and Figure 4-16. 70% of the Public Web Site users connect with private IP addresses. On the other hand, only 20% of the notified users assign private IP addresses. More than half of the

notified users run in a global IP address environment.

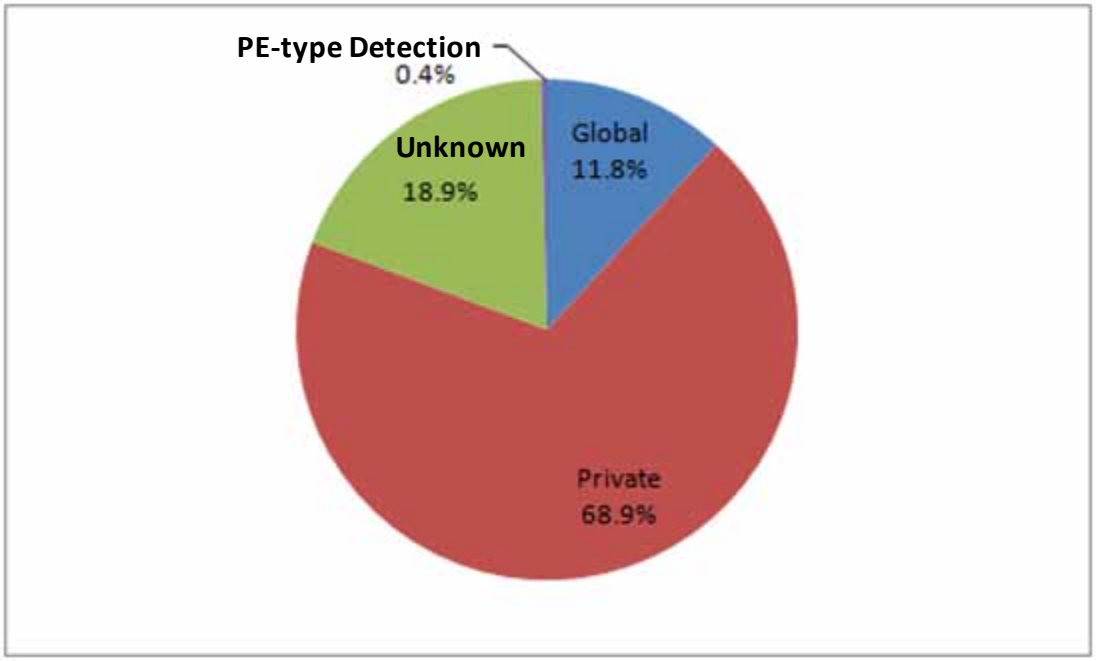


Figure 4-15: Ratio of IP address types (public web site users)

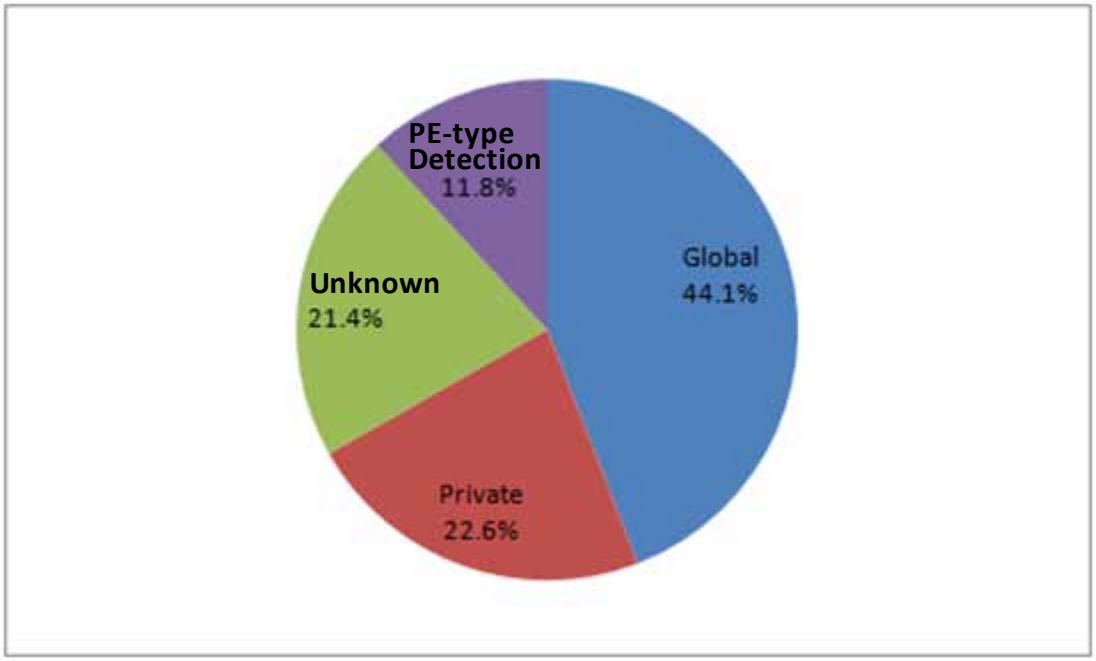


Figure 4-16: Ratio of IP address types (notified users)

⑥ Malware detection ratio by networking environment

The detection rate in each networking environment is shown in Figure 4-17. In the global IP address environment, the malware detection rate was 16%. In the private IP address environment, the detection rate was 10%. The detection rate changes with network environment, also with the state of the operating system and the operating environment of the PC.

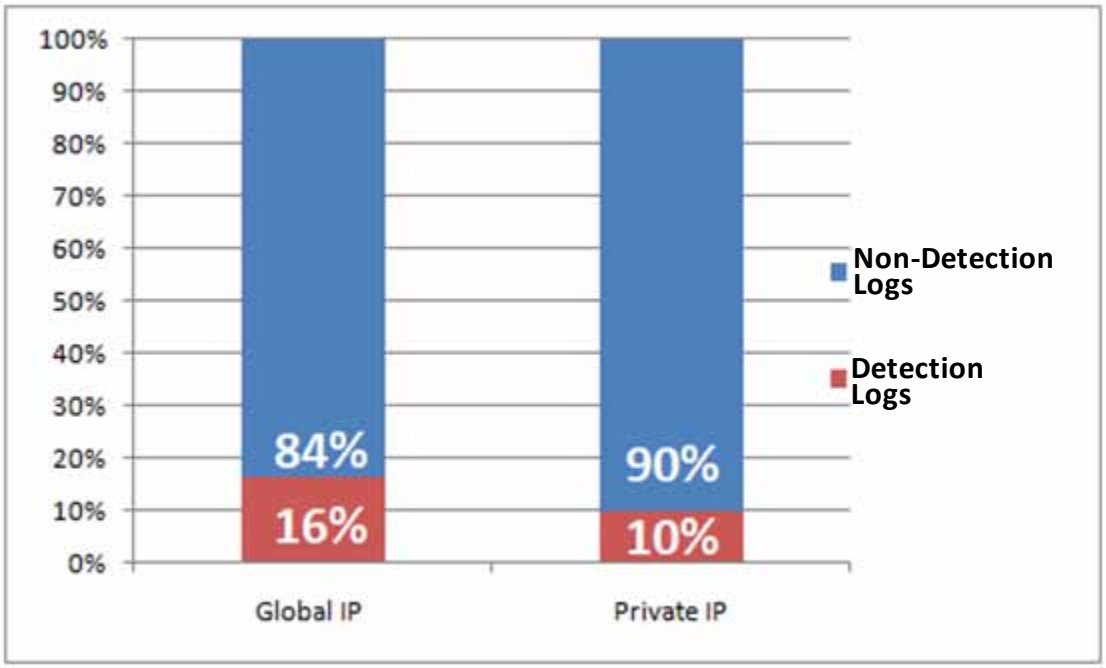


Figure 4-17 Detection rate by networking environment

⑦ Trends in logs over specific periods

For the purpose of investigating the response of notified users, their logs were analyzed from September to December 2009. The results are shown in Figure 4-18 and Figure 4-19. Nearly 70% of users had not maintained the operating system in its latest state (not updated or only partially updated). File infection type malware was detected in many user PCs. It appears that security measures are insufficient in most user environments.

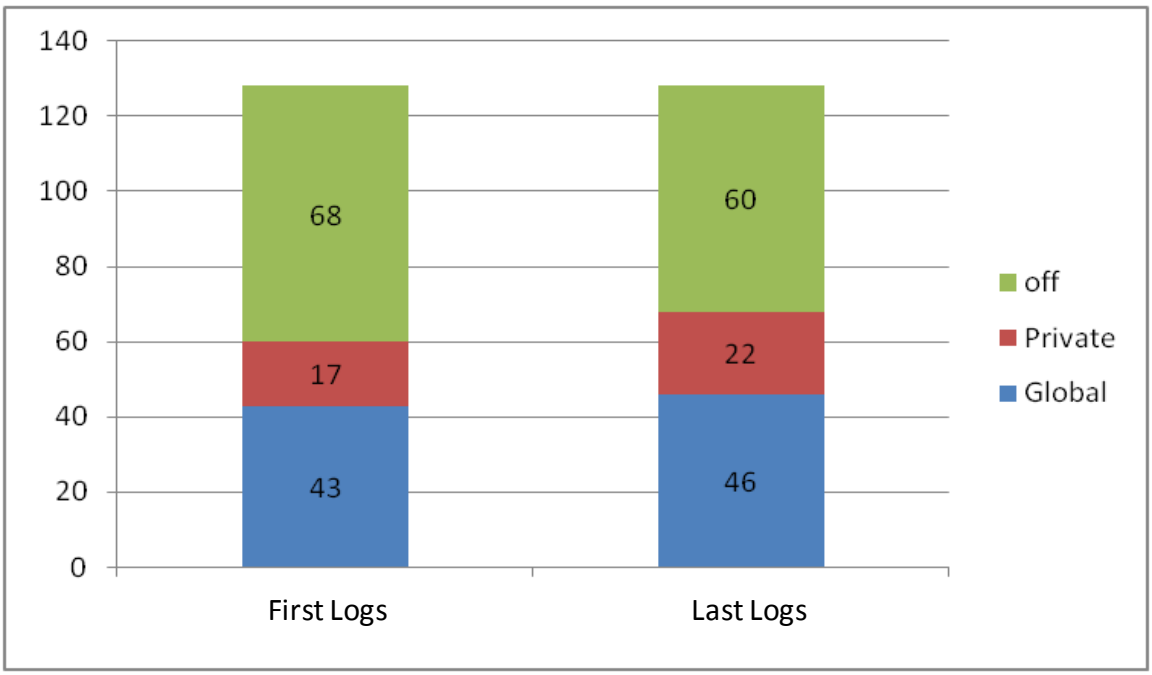


Figure 4-18: Changes in the networking environment

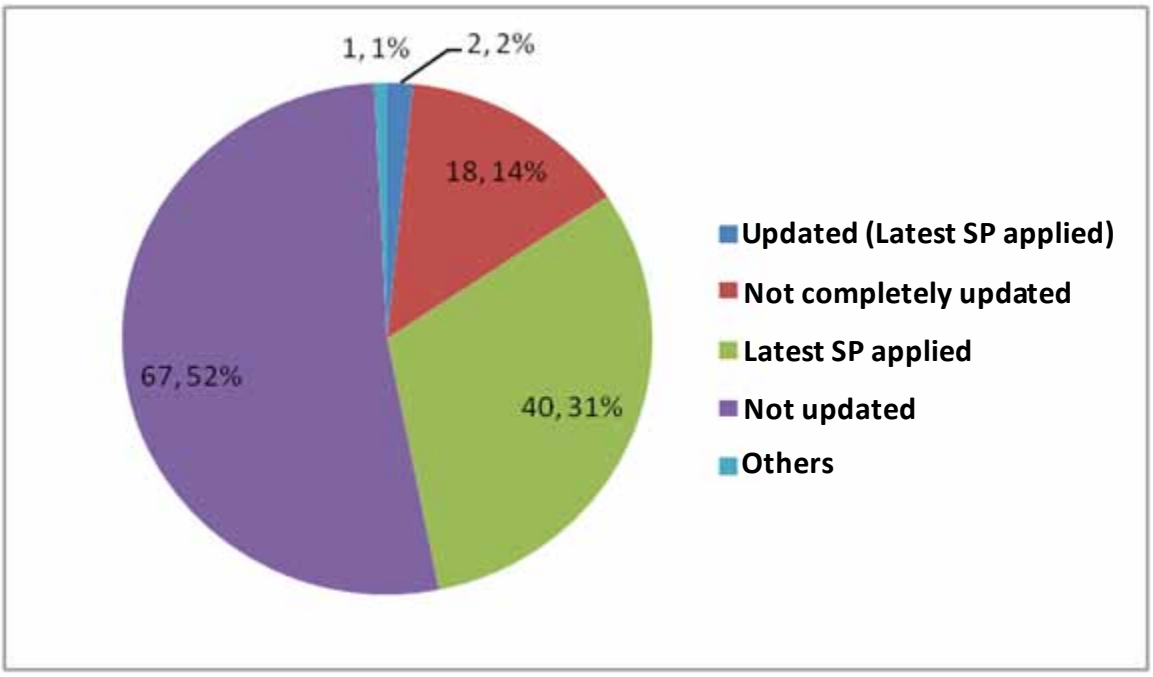


Figure 4-19: OS updates

(2) Log analysis for linkage

In recent years, malware attacking techniques have become more complicated and diverse. There have been some cases in which several malware programs operated in cooperation with each other to complete a series of attacks. It would be difficult to draw a complete picture of such attacks and take effective measures by simply looking at a single sample or the total number of samples.

For this reason, in fiscal year 2009 we investigated the relationships between malware programs and associations between malware and the user environment, to clarify appropriate countermeasures through studying the relationship between the various elements.

① Analysis method

The association analysis method was used to analyze the relationship between malware programs.

Association analysis is a data mining technique that extracts meaningful association rules from a large amount of data. An association rule indicates that if a condition X is provided in a transaction, a result Y occurs. X is called the “conditional part” and Y is called the “result part.” The association rule is represented as:

$$X \Rightarrow Y$$

Let N be the number of data in the transaction, x the data that satisfies the condition X and y

the data that satisfies the result Y. The probability that the rule occurs in the transaction (support) and the probability that the result occurs when the condition is satisfied (certainty) are indicated as:

$$Supp(X \Rightarrow Y) = \frac{x \cap y}{N}, \quad Conf(X \Rightarrow Y) = \frac{x \cap y}{x}$$

② Analysis procedure

The association rules extracted from logs are narrowed into those that represent the following association and are then analyzed:

- Association between malware programs
- Association between operating systems and malware
- Association between network environments and malware

③ Results of analysis

ⅰ） Association between malware programs

Out of the rules on the association between malware programs, those with high certainty are listed in Table 4-2 and Table 4-3. High certainty means that the condition and the result are closely related, suggesting collaboration between malware programs. Support indicates the level of likelihood that a rule occurs, in other words, the extent of the prevalence of the malware combinations.

Table 4-2: Rules indicating association between malware programs (proper names)

Conditional Part	Result Part	Support (%)	Certainty (%)
JAVA_BYTEVER.AC	JAVA_BYTEVER.AB	0.6	100.0
JAVA_BYTEVER.AC	JAVA_BYTEVER.A	0.6	100.0
JAVA_BYTEVER.AB, JAVA_BYTEVER.A	JAVA_BYTEVER.AC	0.6	99.0
JAVA_BYTEVER.AB	JAVA_BYTEVER.A	0.6	97.8
JAVA_BYTEVER.AB	JAVA_BYTEVER.AC	0.6	96.9
WORM_ONLINEG.ZYM	TSPY_ONLINEG.MCL	0.5	96.3
WORM_AUTORUN.DDV	TSPY_ONLINEG.MCL	0.5	94.2
TROJ_QHOST.JM	BKDR_AGENT.GLQ	0.6	91.1
WORM_AUTORUN.DDV, TSPY_ONLINEG.MCL	Mal_Otorun2	0.4	86.9
WORM_ONLINEG.ZYM, TSPY_ONLINEG.MCL	Mal_Otorun2	0.4	86.1

Table 4-3: Rules indicating the association between malware programs (family names)

Conditional Part	Result Part	Support (%)	Certainty (%)
TROJ_GAMETHI, WORM_ONLINEG	Mal_Otorun	1.0	89.1
TSPY_ONLINEG, WORM_AUTORUN, Mal_Otorun	WORM_ONLINEG	1.5	87.5
PE_BOBAX, PE_VIRUT	WORM_BOBAX	1.0	87.5
WORM_ONLINEG,TSPY_ONLINEG,WORM_AUTORUN	Mal_Otorun	1.5	85.7
PE_BOBAX	WORM_BOBAX	1.5	84.8
TSPY_ONLINEG, WORM_AUTORUN	WORM_ONLINEG	1.8	83.4

In Table 4-2, the rules between JAVA_BYTEVER family malware programs are high in both support and certainty. JAVA_BYTEBER is the detection name of malicious Java applets or JavaScripts that use such applets. It is used as the origin of web infection attacks. Its high support indicates this type of web infection is prevalent.

However, no association was found between the malware that is the origin of web infection attacks and downloaded malware (e.g. fake anti-virus software and fake video codecs). This may be because the malware varies widely.

In Table 4-3, the rules that include the WORM_AUTORUN (Mal_Otorun) family and the TSPY (WORM)_ONLINEG family are prominent.

WORM_AUTORUN (Mal_Otorun) is the detection name of the malware that uses removable media such as USB memory sticks as infection media. TSPY (WORM)_ONLINEG is the detection name of the malware that steals online game accounts. Therefore, the purpose of this malware that infects through removable media is the theft of game accounts.

ii） Association between operating systems and detected malware

Out of the rules on Windows XP, those whose certainty exceeds 84.1%, that is, the rate of installation of Windows XP in all logs, are listed in Table 4-4.

Table 4-4: Rules indicating the association between Windows XP and malware

Conditional Part	Result Part	Support (%)	Certainty (%)
TROJ_GAMETHI,WORM_ONLINEG,Mal_Otorun	Windows XP	1.1	99.4
WORM_TATERF, WORM_ONLINEG, Mal_Otorun	Windows XP	1.3	98.9
Cryp_Krap, Mal_Otorun	Windows XP	1.8	98.5
WORM_ONLINEG, TSPY_ONLINEG, Mal_Otorun	Windows XP	2.3	98.4
Cryp_Krap	Windows XP	2.3	98.0
WORM_ONLINEG,TSPY_ONLINEG,WORM_AUTORUN	Windows XP	1.7	97.9
WORM_DOWNAD	Windows XP	2.6	91.5

The online game account theft attacks through removable media, which was found in the association between malware, were detected only for Windows XP. The detection of WORM_DOWNAD also centered on Windows XP.

Out of the rules on Windows Vista, those whose certainty exceeds 6.5%, that is, the rate of the installation of Windows Vista in all logs, are listed in Table 4-5.

Table 4-5: Rules indicating the association between Windows Vista and malware

Functional Part	Result Part	Support (%)	Certainty (%)
TROJ_GETCODEC	Windows Vista	0.3	22.1
TROJ_WIMAD	Windows Vista	0.5	17.9
WORM_ANTINNY	Windows Vista	0.3	13.4
TROJ_FAKEAV	Windows Vista	0.2	13.0
HTML_IFRAME	Windows Vista	0.2	10.4

In the cases of Windows Vista, most detection names were fake video codecs and those that use social engineering,[9] such as P2P, and fake anti-virus software.

Out of the rules on Windows 2000, those whose certainty exceeds 9.1%, that is, the rate of the installation of Windows 2000 in all logs, are listed in Table 4-6.

Table 4-6: Rules indicating the association between Windows 2000 and malware

Functional Part	Result Part	Support (%)	Certainty (%)
TROJ_QHOST	Windows 2000	0.8	28.3
BKDR_VANBOT	Windows 2000	0.5	25.7
TROJ_RANKY	Windows 2000	0.3	23.5
TROJ_PROXY	Windows 2000	0.4	23.2
WORM_KOLABC	Windows 2000	0.3	22.9
WORM_SDBOT	Windows 2000	0.6	21.5
TROJ_DROPPER	Windows 2000	0.4	20.1
WORM_IRCBOT	Windows 2000	0.3	19.9
PE_SALITY	Windows 2000	0.2	18.2

[9] Social engineering is used to acquire important security data, such as passwords, from a PC user using a “social” technique such as conversation, eavesdropping, shoulder surfing, and inducing operating errors.

In Windows 2000, malware that infects through networks are predominant compared to that through removable media or Web sites, which are currently more prevalent.

iii） Association between network environments and detected malware

Out of the rules whose result part is p (indicating private IP address), those whose certainty exceeds 49.0%, that is, the rate of private IP addresses in all logs, are listed in Table 4-7.

Table 4-7: Rules with only private IP addresses and malware names

Conditional Part	Result Part	Support (%)	Certainty (%)
Cryp_Krap	Private IP Address	2.1	90.7
Cryp_Krap, Mal_Otorun	Private IP Address	1.7	90.0
WORM_TATERF, Mal_Otorun	Private IP Address	1.9	87.0
WORM_TATERF,WORM_ONLINEG,Mal_Otorun	Private IP Address	1.1	86.3
TROJ_GAMETHI,WORM_ONLINEG,Mal_Otorun	Private IP Address	0.9	83.6
WORM_TATERF, TSPY_ONLINEG	Private IP Address	0.9	82.3
TROJ_GAMETHI, Mal_Otorun	Private IP Address	1.1	81.8
WORM_ONLINEG,TSPY_ONLINEG,Mal_Otorun	Private IP Address	1.9	81.7
WORM_ONLINEG, Mal_Otorun	Private IP Address	3.1	80.9
Cryp_Nsanti	Private IP Address	0.9	70.1
TSPY_ONLINEG	Private IP Address	3.9	69.0
TROJ_FAKEAV	Private IP Address	0.9	68.9
Cryp_Xed	Private IP Address	1.5	68.8
TROJ_WIMAD	Private IP Address	2.1	67.9
Cryp_Naix	Private IP Address	2.2	66.1
WORM_AUTORUN	Private IP Address	3.5	65.4
WORM_EMBEDDED	Private IP Address	0.7	63.9

In the rules with private IP addresses, removable media infection types were frequently detected. Within this category, the rate of Windows XP is 85.3%. The certainty of the removable media infection rules for Windows XP is nearly 100%. This is why the rate for Windows XP is high.

In addition, the detection names of fake anti-virus software and fake video codecs are prevalent compared to the case with global IP addresses. This trend is noticeable in Windows Vista. However, because of high certainty, it is a specific trend ascribable to private IP addresses.

Similarly, out of the rules whose result part is g (indicating global IP address), those whose

certainty exceeds 15.5%, that is, the rate of global IP addresses in all logs, are listed in Table 4-8.

Table 4-8: Rules with only global IP addresses and malware names

Conditional Part	Result Part	Support (%)	Certainty (%)
WORM_DOWNAD	Global IP Address	1.7	58.1
BKDR_RBOT	Global IP Address	1.0	41.6
WORM_KOLABC	Global IP Address	0.5	39.7
BKDR_SDBOT	Global IP Address	0.5	39.4
WORM_EMBEDDED	Global IP Address	0.4	36.1
TROJ_INJECT	Global IP Address	0.4	30.3
WORM_ALLAPLE	Global IP Address	0.7	30.2
BAT_FTPER	Global IP Address	0.3	29.2
Cryp_Naix	Global IP Address	0.8	22.6
WORM_AUTORUN, TROJ_AGENT	Global IP Address	0.3	21.8
BKDR_IRCBOT	Global IP Address	0.3	21.1
BKDR_VANBOT	Global IP Address	0.4	21.1
TROJ_GETCODEC	Global IP Address	0.3	20.6

In global IP address environments, the detection of WORM_DOWNAD was predominant. In addition, network attack type malware, such as BKDR_RBOT, WROM_KOLABC, and WORM_EMBEDDED, WORM_ALLAPLE were prevalent compared to the case of private IP addresses.

4.3.3. Analysis of collected samples

This section describes the analysis of samples collected with the honeypots operated by the Bot Countermeasure System Operations Group in fiscal year 2009.

(1) Analysis process

As of March 2009, 1,000,082 samples had been collected by the honeypots. It is quite difficult to analyze all of these in detail. Therefore, the Bot Program Analysis Group started with relatively quick methods, such as surface analysis and simple analysis for sampling, then performed in-depth analyses, which resulted in high working efficiency.

The following sections describe each analysis method.

① Surface analysis

The external features of a sample, specifically, various types of file information and the detection name of anti-virus software are identified. This information can be acquired quickly and automatically, and is effective for confirming whether the sample is unique or not.

② Simple analysis

A sample is fed into an automatic dynamic analysis environment, which determines the behavior of the sample and analyzes the results. The whole process is automatic and takes only a relatively short time but there are limitations to the data that can be acquired.

After sampling with the above processes, an in-depth analysis is conducted.

③ In-depth analysis

The sample is disassembled or debugged, and the resulting assembly code is analyzed. In-depth analysis reveals detailed behavior of the sample, including code that is not executed simply by running the sample. In-depth analysis requires analysts with a high degree of expertise and takes an enormous amount of time.

Based on the findings from in-depth analysis, future anti-bot measures are considered.

(2) Analysis results

Similar to fiscal year 2008, the collected samples are narrowed with surface and simple analyses, distinctive samples are then subject to in-depth analysis. A summary of the samples analyzed in fiscal year 2009 is shown in Table 4-9.

Table 4-9: Summary of Samples Analyzed

Number	Characteristics
1	Zeus trojan
2	Encrypted code near the end of the file. The main body is an IRC bot.
3	Written in Delphi.
4	Communicates using HTTP2P.
5	The device driver impairs the operation of DNS.
6	A massive binary combined with a packer. It removes the limitation of the number of TCP connections.
7	The code is expanded in the stack and executed.
8	The created device driver injects a code into svchost.exe.

Number	Characteristics
9	The device driver rewrites SDT.
10	Tampers HTTP. Affiliate.
11	The hook function is divided into drivers and DLLs, which makes it difficult to analyze.
12	Hooks send and recv in Internet Explorer, Firefox, and Opera.
13	Replaces ntfs.sys, injects a code into service.exe and executes it.
14	When unpacked, confuses jump-to using rdtsc. Created with a Borland-C compiler.
15	Creates own copy, rewrites the PE header and turns it into a DLL.
16	An IRC bot that creates autorun.inf.
17	Collects FTP accounts and tampers with Web sites.
18	The packer is created with Delphi and the main body is an HTTP Proxy.
19	The device driver injects a DLL that is written in Delphi.
20	Generates many files, all of which are parts of Mozilla. The main body is written in Visual Basic.
21	Only distinctive characteristic is that character strings are altered so that they are difficult to read.
22	Rewrites cdrom.sys and turns it into a device drive that injects a code.
23	File infection type.

The above samples have the following functions:

- Collecting FTP accounts and using them to tamper with Web sites
- Collecting e-mail addresses and sending spam mail
- Performing DoS attacks
- Displaying an affiliate site and automatically accessing it
- Performing encrypted communication with OpenSSL
- Covering up various information and operations with kernel mode malware
- Tampering with communications by kernel mode malware
- Analysis-resistant function

Some of the distinctive features are as follows.

① Functions exploiting vulnerabilities

In the samples analyzed in fiscal year 2009, there was one that tried to raise its privileges by exploiting vulnerabilities. The target vulnerabilities are listed in Table 4-10

Table 4-10: Exploited vulnerabilities

Security Information Number	Description
MS08-025	Privilege can be raised due to the vulnerability of the Windows kernel.
MS08-066	Privilege can be raised due to the vulnerability of the Microsoft Ancillary Function driver.

The function may be intended to execute arbitrary codes at the kernel privilege by circumventing access controls, such as the limited user in Windows Vista and Windows XP.

② Spread of analysis-resistant functions

Analysis-resistant functions, which have been witnessed before, were prevalent in the samples in fiscal year 2009. Those functions are listed in Table 4-11.

Table 4-11: List of analysis-resistant functions

Item	Description
PCI Bus Investigation	Investigates the IDs of the devices connected to the PCI bus and detects virtual machines.
IDTR Investigation	Investigates the value of the Interrupt descriptor Register (IDTR) and detects virtual machines.
User Name Investigation	Investigates whether the user name is that of sandbox or vmware, and detects a dynamic analysis environment.
API Return Value Investigation	Calls an API with an illegal argument and detects a dynamic analysis environment by its return value.
DNS Response Investigation	Resolves the name of a certain domain, matches its IP address with the proper address stored by itself, and detects a dynamic analysis environment.
Code Injection	Impairs dynamic analysis and the detection of malware by injecting a code into another process.
Character String and Data Processing	Processes a character string and data, and decodes it when used to impair static analysis.
Making Codes Difficult to Read	Impairs static analysis by injecting useless instructions into the code.

The above functions have been witnessed before. However, in fiscal year 2009, two-thirds of the samples analyzed had one of the functions in Table 4-11. Therefore, these functions will be implemented as standard.

③ Functions making communication difficult to intercept

An in-depth analysis was conducted on the samples observed in late fiscal year 2008 that perform OpenSSL-encrypted communication in HTTP and P2P environments. It is estimated that the HTTP circumvents firewalls, OpenSSL encryption impairs the analysis of communication, and P2P hides the creator and herder and improves availability. It has been clear that the samples that have this function are the same type as the bots downloaded by Web infection attacks (so called “Gumblar”) seen in late fiscal year 2009.

These samples sometimes represented as “HTTP2P.” It allows communication between malware programs through the following steps:

i） URLs (e.g. http://192.0.2.1/xrhlb.png) are generated from a large list of IPs (i.e. default peer list) and random character strings.
ii） The XML data actually used in communication is encrypted using the default certificate of OpenSSL.
iii） The encrypted data is sent to the URL generated using the POST method.
iv） Encrypted data is similarly received.

The following types of communication are performed using encrypted data:

- Authentication to connect with the target party
- Sending and receiving commands
- Sending spam mail
- Sending and receiving the data required for sending spam
- Downloading files and executing them
- Updating own files
- Performing DoS attacks
- Updating the peer list and applying various access controls

④ Spread of kernel mode malware and sophistication

In fiscal year 2009, there were many samples that generated kernel mode malware, such as rootkits. Kernel mode malware has been growing in number since late fiscal year 2008. Their main functions are those of rootkits, such as hiding files and processes. An in-depth analysis revealed that some samples have more sophisticated functions, as well as hiding files and processes.

- Manipulating files without using APIs
- Sending and receiving TCP without using WinSock

These functions directly interact with the device driver omitting the standard procedure used by applications. The purpose of this may be to avoid or impair analysis, hiding itself, and

eliminating the effects of filters. Implementing these functions requires a high level of expertise, which suggests the rising skills of malware creators.

Some samples tamper with user communications by using filter driver technology. This type of malware will spread because the development cost of kernel mode malware will decrease through using filter driver technology.

4.3.4. Review of measures

In fiscal year 2009, a study on the countermeasures proposed based on the results of analyses conducted in fiscal year 2008, and a review of the countermeasures based on the results of analyses conducted in fiscal year 2009 were undertaken.

(1) Study on coordination for closing malware distribution sites

① Background

According to in-depth analysis in fiscal year 2008, the sites distributing malware were providing samples of the same functions with different hashes. The purpose of this may have been to avoid detection by anti-virus software. They always used certain kinds of tools to prevent the malware from being detected by anti-virus software.

These malware distribution sites exploit the opportunity period before corresponding pattern files are created by anti-virus software developers. To address the problem of these sites, one possibility is to demand ISPs deactivate such sites (coordination for closing sites). A survey on coordination for closing sites was conducted in fiscal year 2009.

② Survey areas

Canada, United States, Russia, and Eastern Europe

③ Outline of the survey

Hearings were conducted in six categories for security-professionals in each area:

i) Cyber security in general
ii) Capturing bots using honeypots
iii) Activities such as distributing disinfection tools and vaccines
iv) Coordination with the abuse contacts (service desks) of ISPs
v) Coordination for closing malware distributing sites
vi) Coordination for black-listing malware distributing sites

④ Summary of the survey

i) Canada and United States

The ISPs in Canada and the United States take anti-bot measures. Similarly to the CCC, they analyze the behavior of bots and operate honeypots or honeynets for early detection. To identify the users of bot-infected PCs, they also analyze network traffic, capture

communications to the ports known to be used by bots, and detect the peculiar behavior seen in the early stages of infection.

However, these activities are conducted by individual ISPs. Activities like the CCC's anti-bot measures with cooperation from ISPs are not undertaken in Canada or the United States. We think that this is because of the following reasons:

1) Security measures and tools

There is a perception that security measures should be provided to the customer as a service, and tools such as honeypots are means to increase the superiority of the services and should not be distributed for free or even shared.

2) Sharing information

There are regulations on the sharing of customer information and Personal Identifiable Information (PII)[10] from the viewpoint of the guarantee of privacy. ISPs could provide information on the behavior of bots but such a provision is performed within the legal limits and based on a business-like relationship.

3) Abuse[11] contacts (service desks)

They are basically cost centers, most of which are subcontracted. ISPs tend to limit customer relations efforts.

4) Measures against malware distributing sites

The basic measures against malware distributing sites are legal formalities including lawsuits by persons or companies. If laws and regulations of each country require submission of certain kinds of records to the law court, ISPs follow them. However, they tend to avoid such measures due to the cost, etc.

No cooperation is established between ISPs simply for common interest unless some business benefit is expected or there is a legal requirement. Measures similar to those taken by the CCC would be difficult to implement.

Those security measures requiring international cooperation are mainly conducted by the National Computer Security Incident Response Team (National CSIRT)[12] and the Forum of Incident Response and Security Teams (FIRST).[13] In Japan, JPCERT/CC is the organization responsible for international cooperation.

---

[10] Indicates personal information.
[11] The contact of an ISP to which Internet-related nuisances and other such problems are reported.
[12] The name of the organization that receives reports on computer security problems, investigates them, and takes appropriate measures.
[13] The name of the international organization of the CSIRT that receives reports on computer security problems, investigates them, and takes appropriate measures.

ⅱ） Russia and East Europe

In Russia and East Europe, anti-bot measures are basically conducted by individual ISPs. The CCC's type of anti-bot measures with cooperation from ISPs is not currently performed.

However, during an interview, a Russian professional told us that in a meeting of Russian ISPs, the Japanese anti-bot activities were discussed and similar efforts by private companies were suggested.

Details of those efforts are currently not known, but if they undertake such activities in the future, our example might serve as a starting point.

⑤ Discussion

According to the results of the study, we think that it is more effective to enforce the existing cooperation for managing incidents (cooperation between FIRST and the CSIRTs of different organizations) to establish coordination for closing sites rather than to conduct such coordination as an activity of the CCC.

(2) Review of the measures to be taken based on the results of the analyses in fiscal year 2009

From the results of the analyses in fiscal year 2009, the following trends can be estimated.

- Spread of linking to malicious Web sites and raising privileges by exploiting vulnerabilities
- Spread of sophisticated kernel mode malware
- Spread of encrypted and P2P-type communications

Since Windows Vista and later operating systems apply more strict access control such as UAC, there will be more social engineering methods to persuade PC users to execute malware. Then local vulnerabilities are exploited to raise privileges so that the malware can do anything it wants on the infected terminal.

Combining encrypted communication and hiding files and processes makes it more difficult to detect malware. And, with the P2P communications, it could be impossible to reach the malware creator or manager.

① Measures to be taken at the level of general PC users

The following measures should be taken by general PC users:

- Use of a private IP addresses
- Updating the operating system and application software
- Upgrading the operating system
- Being aware of social engineering issues

In the analysis of the logs, considering the trend of infection in a networking environment, the risk of using a global IP address was confirmed. It is necessary to introduce a broadband router or other means to avoid directly connecting the PC to the Internet.

In particular, mobile terminals are frequently assigned to global IP addresses, and so it is necessary to educate the public about such threats.

The risk of not updating the operating system and applications has been confirmed with the results of analyzing the samples as well as logs. This issue has also been repeatedly raised in public.

With SP application checking by the CCC Cleaner and public education by the CCC on its Web site, increasing numbers of general PC users recognize software updates as anti-bot measures. Public education activities should be continued.

Upgrading the operating system does not only serve as a measure against attacks currently prevalent according to the results of association analysis, but is also effective for kernel mode malware because sophisticated access controls, such as UAC and driver signatures, are implemented. It is preferable to encourage general PC users to upgrade their systems.

Considering the expected occurrence of fake anti-virus software that will be difficult to distinguish due to localization, awareness of social engineering issues needs to be raised.

② Sophistication of analysis technology

The analysis of malware is indispensable for planning countermeasures. In particular, to cope with malware using continuously sophisticated techniques, it is necessary to improve the sophistication and efficiency of the analysis technology.

Specifically, the following analysis techniques need to be established:

- Simple analysis of kernel mode malware
- Unpacking technology including kernel mode malware
- Simple decoding and collection of processed character strings and data
- Simplify codes that have been made difficult to read
- Virtual environments that more closely emulate real machines
- Improving the capacity of analysts and their training
- Sharing analysis information
- Speeding up in-depth analysis with real time analysis using several people

③ Measures taken within a larger framework

It is considered to be effective to reduce the number of bot creators as well as the users of bot-infected PCs. In Japan, it is desirable to establish a law that punishes the creation and distribution of malware.

Today the ultimate purposes of bots are in many cases financial, including sending spam,

guiding the user to affiliated sites, and performing DDoS attacks. Therefore, in addition to taking measures from the viewpoint of general PC users, or the targets of infection, and analysts, raising the costs for attaining their goals could reduce the number of bot creators.

More specifically, the following efforts may be effective:

- Spreading anti-spam technology such as SPF and OP25B
- Developing the technology for protecting affiliated sites
- Studying DDoS countermeasures

Since malware activities cross national borders, international cooperation in taking preventive measures and addressing incidents is required. Therefore, we should strengthen international coordination and collaboration among the relevant organizations concerned.

4.4. Future plans

In fiscal year 2010, the efforts of fiscal year 2009 will be continued with the aim of sophisticating, stabilizing, and bringing increased efficiency to our activities.

(1) Creating the CCC Cleaner

Analysis of collected samples will be continued and the CCC Cleaner will be effectively distributed.

(2) Analyses of bots

Based on the activities in fiscal year 2009, bot analysis with new approaches will be conducted seeking the estimation of future threats and develop necessary countermeasures.

(3) Public education

Similar to fiscal year 2009, public education on anti-bot measures will be undertaken.

Phased privatization of the activities and alternative methods to the CCC Cleaner will be discussed.

5. Activities of the Bot Infection Prevention Promotion Group

5.1. Outline

With the aim of augmenting bot infection prevention measures taken by general PC users and avoiding reinfection, the Bot Infection Prevention Promotion Group is working on a project in cooperation with security vendors. Specifically, they provide vendors of infection prevention measures with bot samples collected by this project so that they can be reflected in the development of pattern files for anti-virus software sold by such vendors.

When PC users update the pattern files of their anti-virus software, the bots collected in these projects can be detected and disinfected, which should improve the level of security measures.

5.2. Vendors of infection prevention measures

The security vendors participating in this project are legally-defined bodies who have set up strict standards for managing samples, have analysis divisions in Japan, and have a proven track record in providing anti-virus software and services in Japan.

These security vendors are called infection prevention measures vendors, who promote infection prevention measures for PCs.

Infection prevention measures vendors (in alphabetical order)

- AhnLab, Inc.
- Kaspersky Labs Japan
- McAfee, Inc.
- Microsoft Corporation
- SOURCENEXT Corporation
- Symantec Corporation
- Trend Micro Incorporated

5.3. Results of activities

Table 5-1 shows how the infection prevention measures vendors reflected the samples acquired from this project in the pattern files of their anti-virus software from March 2009 to the end of March 2010 (reporting months: May 2009 to April 2010). The table categorizes the status of reflection as “Already Reflected” (the samples had already been detected before they were provided from the project); “Reflected from the Project” (the samples were reflected in the pattern file); and “Not Reflected” (the samples were not reflected in the pattern file), and lists the average rates among vendors.

Table 5-1: Reflection of Samples in Pattern Files

Reflection	Average in Fiscal Year 2009
Already reflected	96.5%
Reflected from the project	2.7%
Not reflected	0.8%

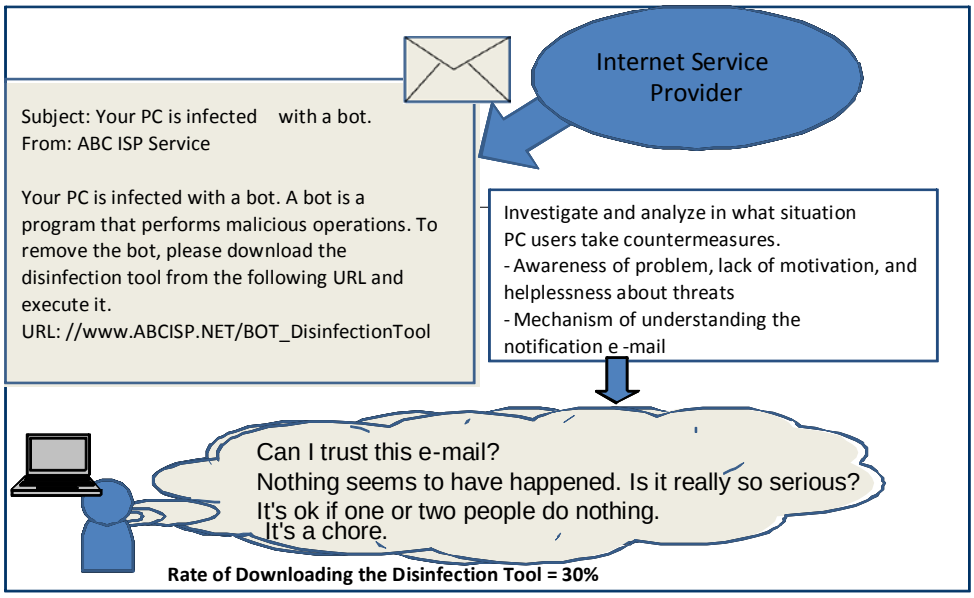
The rate of 99.2% that is the total of “Already reflected” and “Reflected from the project” indicates that 99.2% of samples collected in this project can be detected by anti-virus software. This number is one of the achievements of this project and proof that the samples have served a purpose and contributed to preventing PCs from becoming infected with bots.

5.4. Future activities

We will continue strict management of collected samples and collaboration with security vendors so that the samples are reflected in the development of pattern files for their anti-virus software.

Column: Bot assessment and human behavior

Since bots seldom causes problems on the infected PCs, users do not always realize the damage being inflicted by their PCs. For this reason, some users think that there is little benefit in taking anti-bot measures. The Information-Technology Promotion Agency (IPA), Japan is conducting a survey on the reason why the rate of users who take anti-bot measures is low from the viewpoint of personal decision-making mechanisms. Decision-making has long been studied in the social science field.



The purpose of the survey is to clarify what procedures are effective for promoting anti-bot measures by exploiting findings in this field. The survey was carried out in the form of a web questionnaire. It

examines “recognition elements,” such as "how the user estimates personal damage (caused by bots)"; "how the user recognizes the effects of taking measures"; "what the user thinks of the time and labor taken to implement measures"; and "if the user believes the measures are effective for the entire network, including the ISP." The survey results indicate that 80% of notified users believe that they should take anti-bot measures, and the time and labor taken are not significant. And the stronger the feeling of the risk of their PCs suffering from bots, the higher the intention to take measures becomes. Therefore, to motivate users to implement anti-bot measures, it is necessary to reduce the time and labor, and increase the feeling of risk.

Then, exploiting the "psychology of persuasion," they are investigating the behavior of users when they are notified of a threat. The purpose of the investigation is to determine what form of message most leads the user to take measures. The results of the investigation are expected to tell us what types of messages we should send to promote security measures. This survey was also conducted in the form of a Web questionnaire. It has become clear that when the users receive a message that informs them about the "effects" of such measures, they are more active in taking measures. Many of them do not understand the technical details when implementing such measures, and are greatly influenced by the reliability of the sender (i.e. ISP) and reports by the media. In conclusion, for threats like bots that inspire less risk of becoming victims, the time and labor taken to implement measures should be reduced and the message needs to indicate not only the risk but the effects of the measures in a distinctive form. In addition to questionnaires, the IPA also conducted psychological experiments. Through these efforts, it is expected that specific guidelines for creating effective messages will be developed. The activities of the IPA are introduced in the following URL. They have also reported their activities in the "RSA Conference TOKYO 2010" and the "Information Security and Behavioral Science Workshop" held by the IPA since 2009.

6. Efforts across groups

6.1. Fostering malware specialists

In addition to the direct anti-bot measures that identify and notify the users of bot-infected PCs, the three groups of the Cyber Clean Center (CCC) support the fostering of anti-malware specialists from a broader perspective.

The reason why the CCC does this is that anti-malware measures are not short-term quick fixes but need to be conducted with a medium-to-long term view, for which it is indispensable to foster human resources for the future.

This section describes two efforts the CCC has been making: IT Specialist Program to Promote Key Engineers as Security Specialists (IT Keys), and Malware Specialists Fostering Workshop (MWS).

(1) IT Keys

The IT specialist program to promote Key Engineers as security specialists (IT Keys) is one of the programs conducted by the Ministry of Education, Culture, Sports, Science and Technology (MEXT) for fostering advanced IT specialists. Four IT graduate schools (Nara Institute of Science and Technology, Osaka University, Kyoto University, and the Japan Advanced Institute of Science and Technology), and four companies and organizations (National Institute of Information and Communications Technology, The Research Institute of Information Security, JPCERT Coordination Center, and NTT Communications) combine their forces and collaborate in their expert education programs and real environment training programs. The purpose of their efforts is to foster specialists with hands-on skills, including knowledge and common-sense backed by experience, as well as multifaceted and all-around competency for playing a leading role in resolving information security problems.

The CCC has been carrying out IT Keys risk management exercises since fiscal year 2008. They include seminars on CCC activities, analysis exercises, security vendor tours targeting the freshmen in the master's courses of the above four universities. The environments and programs for the risk management exercises were designed and built based on the experience of the CCC.

Periods

September 16 to 19, 2008 (four days)

September 15 to 18, 2009 (four days)

Major Activities

Bot Infection and Analysis Exercise (Conducted by the Bot Countermeasure System Operations Group)

Static Analysis Exercise (Conducted by the Bot Program Analysis Group)

Changes in Viruses and Other Threats in Networks and Countermeasures (Conducted by the Bot Infection Prevention Promotion Group)

(2) MWS

The Malware Specialists Fostering Workshop (MWS) is a workshop activity that has been held by the Information Processing Society of Japan (IPSJ) and the CCC since fiscal year 2008. The purpose of the workshop is to foster researchers and practitioners with expert knowledge in malware.

The MWS uses the CCC DATAset (a research data set comprising three types of bot data collected by the CCC: malware hashes, attack communication data, and attacker data) to enable "sharing the results of research," and provide the means for "brushing up skills" and "publishing the results of academic research."

Periods
MWS2008：October 8 to 10, 2008 (Okinawa)
MWS2009：October 19 to 21, 2008 (Toyama)
Hosts
Cyber Clean Center-Steering Committee (CCC-SC) and Information Processing Society of Japan (IPSJ)

One of the features of MWS（MWS2008/MWS2009） is that the researchers can share the results of research because they analyze the same research data set provided by the CCC. As each researcher uses a different analysis process, the results may differ.

The results of research are reported in the workshop so that practical knowledge is shared among the researchers, which helps fostering security researchers, setting a goal for improving skills, finding advanced subjects of research, and evaluating and fostering researchers.

In MWS2009, a unique program, the MWS Cup was held. The participants analyzed the "CCC DATAset" within a limited time, and answered questions on attack communication data and malware names. The scores were marked based on three categories: Technology, judged according to the number of correct answers; Art, judged by reviewing analysis techniques; and Overall, that is the total of technology and art. For each category, a Technology Prize, an Art Prize, and the Overall winners were awarded.

The contents of research correspond to the observation data groups in the research data set (CCC DATAset). The relationship between bot-infection attacks and the contents of research is shown in Figure 6-1.

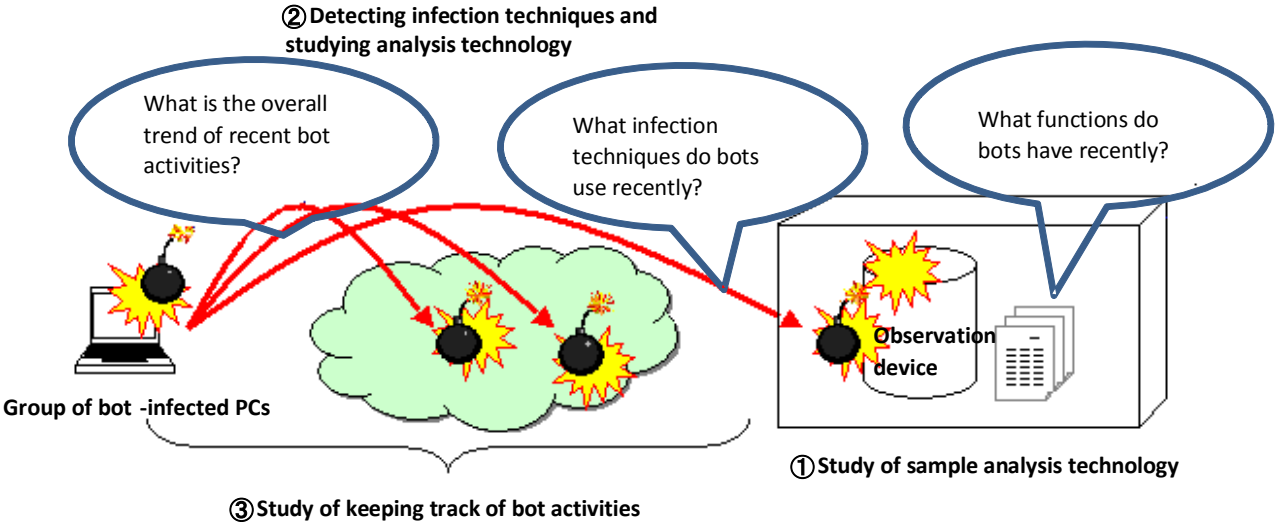


Figure 6-1: Relationship between various fields of study and CCC DATAset

① Research on sample analysis technology (malware hashes)

This research uses the malware hashes collected by honeypots to create a research data set. The hashes were narrowed down to those of the malware for which the results of analysis can be collated, those of several types of malware for which associations can be analyzed, and those of malware that were of technical importance, such as distinctive functions.

② Research on the detection of infection methods and analysis technology

This research uses full-captured communication data acquired by the observation devices used for creating the research data set.

③ Research on the technology for keeping track on bot activities (attacker data)

This research uses the log data for the malware acquired by the observation devices used for creating the research data set. It includes the time at which the malware was acquired, source IP address, source port number, destination IP address, destination port number, TCP/UDP, hash (SHA1) of the malware sample, virus name, and file name.

6.2. Collaboration with mass media

The Cyber Clean Center (CCC) has been working to eliminate bots and avoid reinfection by collaborating with ISPs in notifying the users of bot-infected PCs. Those efforts are covered by various media, which has promoted public awareness of anti-bot measures.

CCC activities have revealed that most of the bot-infected PC users had not implemented sufficient security measures. There were also many users who were unwilling to take measures even if they received several notifications. The role of the CCC is to find the users of bot-infected PCs, notify them,

and provide them with specific countermeasures. However, it is the PC users themselves who must actually institute the anti-bot measures. Therefore, practical activities for raising the awareness of individual PC users are indispensable.

It has become evident that collaboration with the mass media is effective in promoting anti-bot measures. The trend in the number of downloads of the CCC Cleaner on the Public Web site is shown in Figure 6-2.

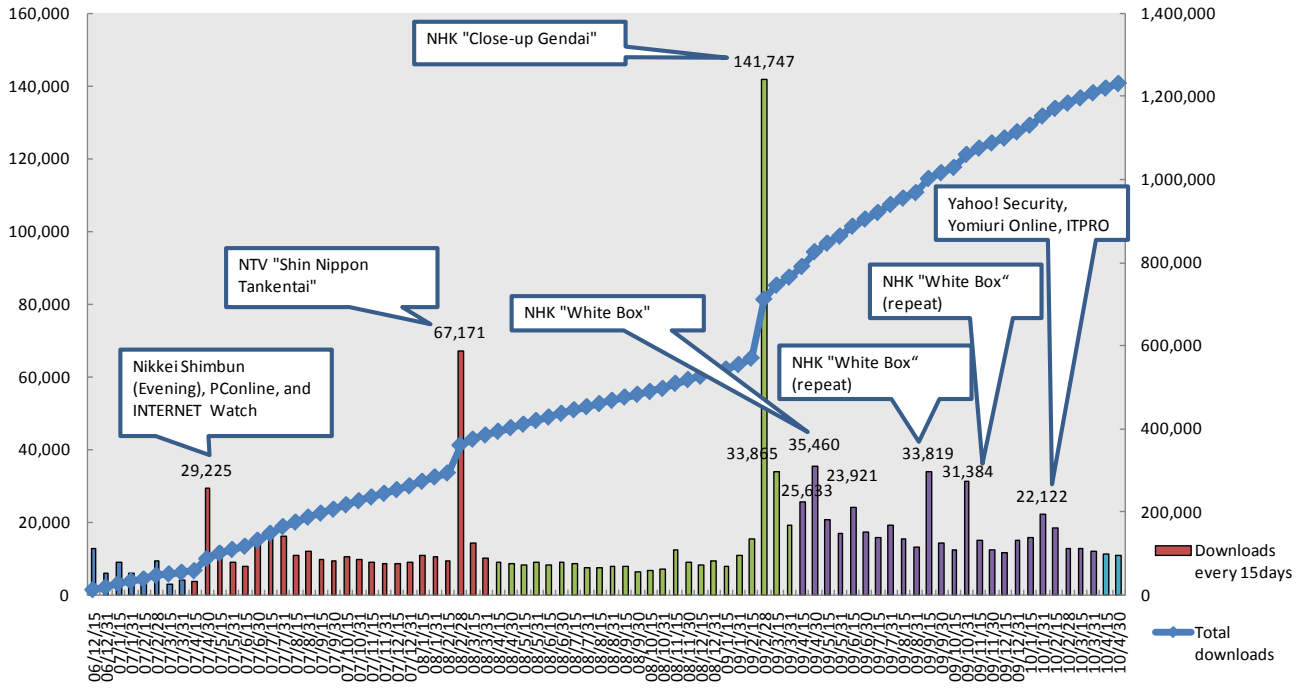


Figure 6-2: Trend in the number of downloads of the CCC Cleaner at the Public Web Site

Since the establishment of the CCC, each time CCC activities are covered by the mass media, the number of accesses to the Public Web Site increased, and the number of downloads of the CCC Cleaner exceeded the usual level. This indicates that media coverage enhances recognition of the CCC, which leads users to download the CCC Cleaner. This also implies the possibility of reaching users of infected PCs who are “not aware of” the e-mail notifications from the ISPs, and the users of infected PCs that could not be detected by the honeypots. We intend to continue active cooperation with the mass media to educate general PC users about anti-bot measures.

6.3. Need for international coordination

Bot infections spread across national borders. Even if the number of bot-infected PCs decreases and infection attacks from Japan have been eliminated, infection attacks from bot-infected PCs will never stop unless the number of bot-infected PCs also decreases in other countries. The number of attackers’ IPs by country collected by the attack event collecting honeypots is shown in Figure 6-3. This chart indicates that 75% of attacks originate overseas.

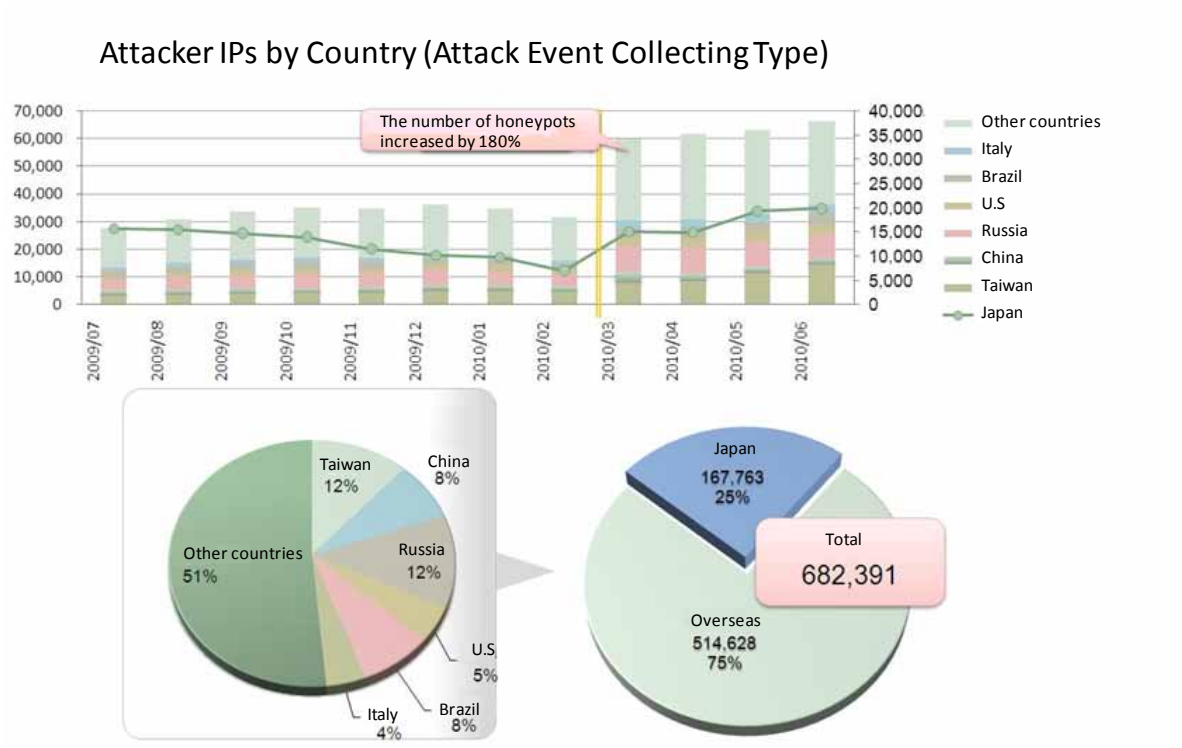
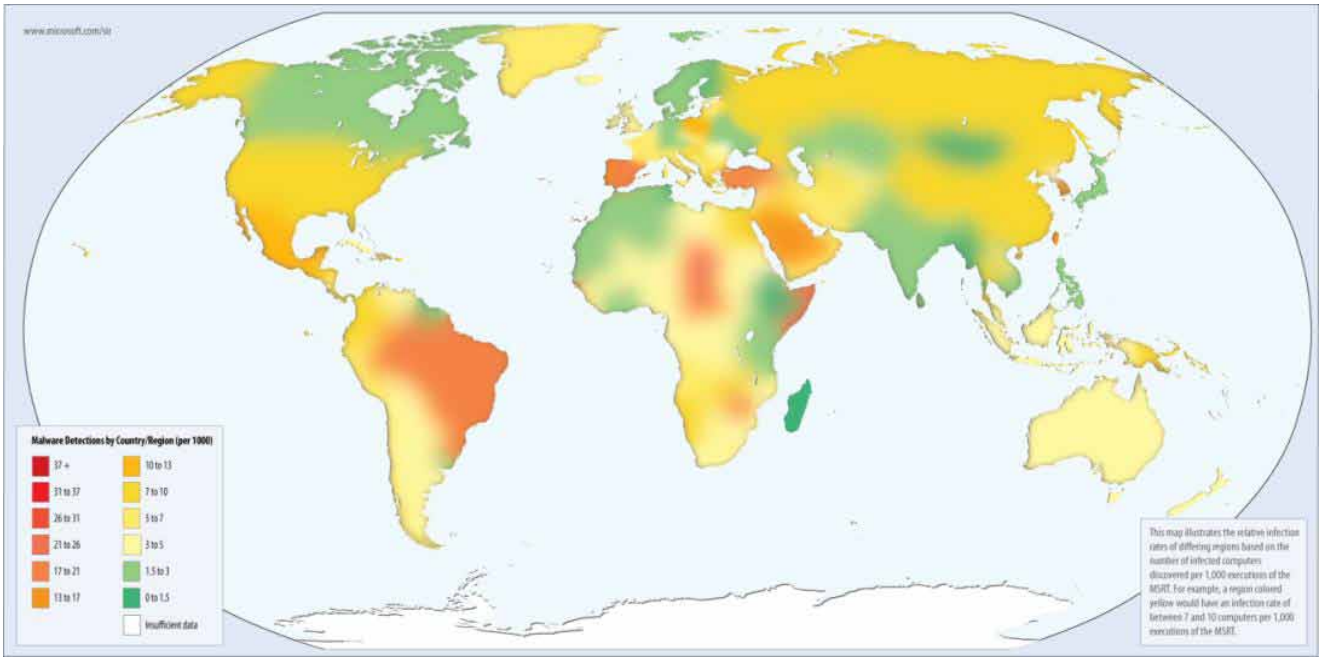


Figure 6-3: Trend in attackers' IPs by country collected by attack event collecting honeypots

As the number of honeypots was doubled (from 20 to 40) in March 2010, the number of collected attack events increased both domestically and from overseas. The ratio between domestic and overseas has hardly changed. According to "Microsoft Intelligence Report July – December 2009" (infection rate by nation) published by Microsoft Corporation, the infection rate of Japan is very low on the worldwide scale.



Source: Microsoft Security Intelligence Report 2009 July – December 2009

Figure 6-4: Infection rate by country

To keep the bot infection rate low in Japan, it is important to suppress infection from overseas. This requires the establishment of an international coordination scheme that realizes anti-bot measures from the global viewpoint.

7. Anti-bot measures to be taken in the future

This chapter proposes the minimum anti-bot measures that should be implemented by individual PC users and the procedure for preventing the spread of bot infections in the future.

(1) Introduction of a broadband router

In a configuration without a broadband router where a PC is connected directly to the Internet, if there is a systematic defect or specification issue in the operating system or an application, the PC could be infected in several minutes.

If the PC is connected to the Internet through a broadband router, the NAT function of the router avoids infection attacks from outside, resulting in a safe and infection-resistant environment.

Reference: Effectiveness of a broadband router (infection survey by line and by region)

The rates of infection blocks (/16) by line and by region were surveyed on three ISPs. For FLET'S ADSL, samples were captured for three companies with no regional dependency. For FLET'S Hikari, the rates of infection blocks in the NTT West area were lower for three companies.

This is because NTT East and NTT West have different policies in providing access lines. NTT West provides two types of optical access lines: Family 100 and Hikari Premium. The latter requires a router. Further, Hikari Premium has larger customer base. Thus the field data also shows that a router protects the PC from infection attacks from the Internet. A router is thus an effective tool for preventing bot infection.

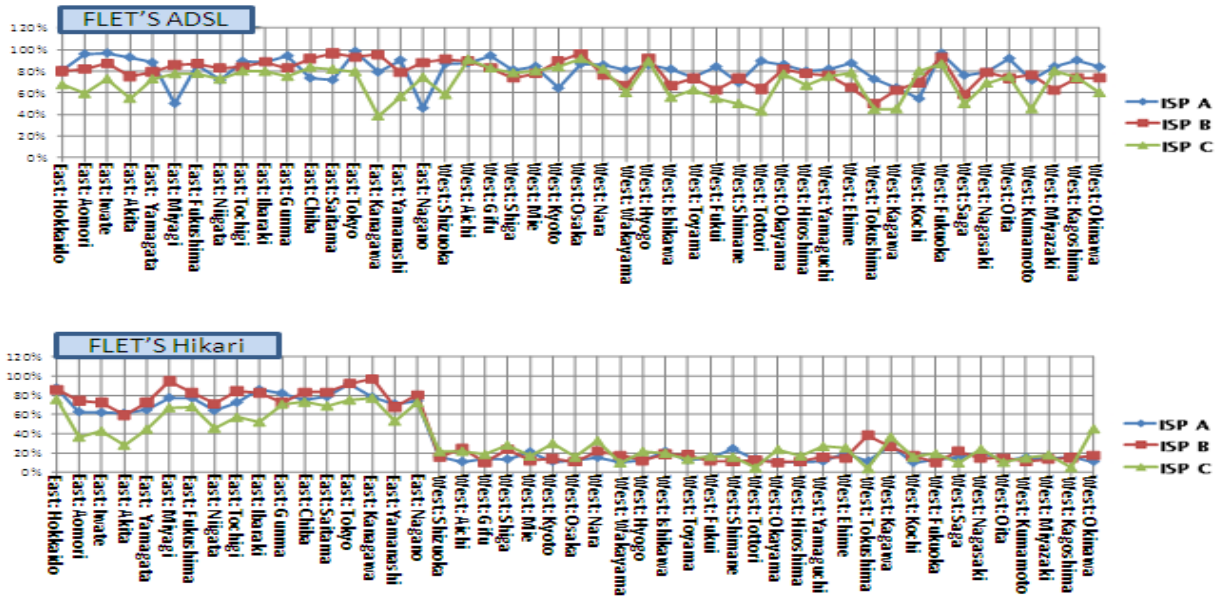


Figure 7-1: Detection rates of infection blocks (/16) by line and by region

(2) Updating the operating system and applications

When a security hole is found in Windows or other operating system, or in an application program, the developer usually issues a fix.

Since security holes are frequently the causes of virus infection and an abuse of a PC, it is very risky to leave such security holes unfixed.

As Windows security holes are often the target of bot attacks, Microsoft Corporation recommends running Microsoft Windows Update at least once each month.

Recently, there has been malware that exploits the security holes of applications such as Acrobat Reader (PDF viewer), Adobe Flash Player, Java Runtime Environment, and Microsoft Office. Therefore, in addition to updating the operating system, it is also important to keep these applications in the most up-to-date state.

(3) Introduction of anti-virus software

There are various security risks on the Internet. Using the services on the Internet exposes the PC to the risk of being infected by computer viruses. Using anti-virus software mitigates such risks.

Even if anti-virus software has been installed, when the virus definition file has expired or regular updates have not been performed, the software cannot cope with new viruses. It is important to keep the anti-virus software up-to-date, and regularly run virus scanning to confirm that the PC is clean.

(4) Suggestion of port blocking

Bots are known to infect other hosts using certain TCP/UDP ports. Specifically, many bot infection cases involve TCP/UDP ports 135 to 139, and 445, which are used by the Windows file sharing service. Blocking these ports is effective for preventing the spread of bot infections.

The CCC conducted a survey on preventing the spread of bot infections by blocking certain ports, and has confirmed that the spread can indeed be controlled by blocking certain ports. The trend in the number of bot samples collected by ports blocked and the number of logs indicating dropped attack events for the two months from April 8, 2010 is shown in Figure 7-2.

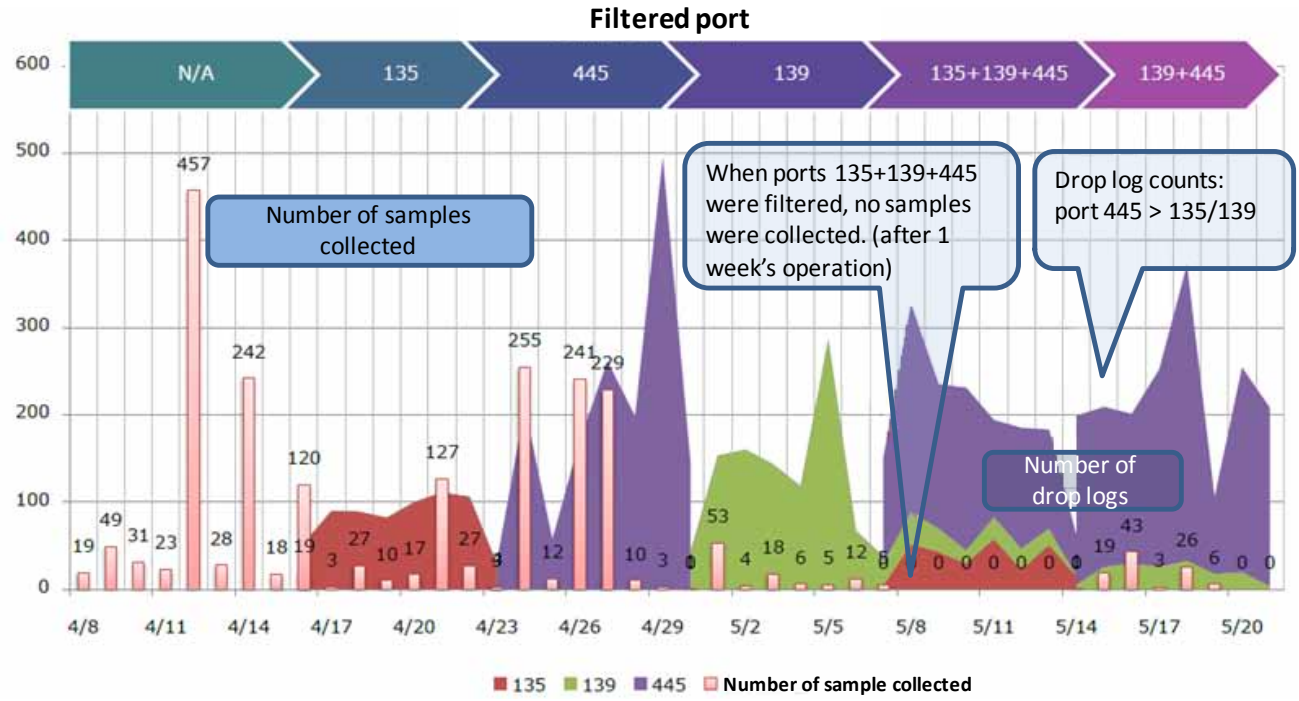


Figure 7-2: Effect of port blocking by port

For the week commencing April 8, no port was blocked and attacks on the honeypots were checked. Then observations were conducted using the following three cases: (1) blocking ports 135, 445, and 139 individually; (2) blocking ports 135, 445, and 139 simultaneously; (3) blocking ports 139 and 445 simultaneously. Each bar in the chart indicates the number of samples collected. Blocking a single port decreased the number of samples. However, when the three ports were blocked together, no samples were collected during the specified period.

Blocking certain ports is highly effective for preventing the spread of bots. We would like to propose this as one method among various anti-bot measures.

Port blocking can be performed by PC users by setting up a broadband router or firewall. However, it is unlikely that all PC users can properly apply port blocking. Port blocking by the ISP can prevent the spread of bot infection to all users.

However, since port blocking by an ISP could be an infringement of the confidentiality of communications under the current legal system, legal reform is required. We must thoroughly discuss this issue by confirming that blocking certain ports does not impair the convenience of users and poses no problem for ISP operations.

8. Summary

The Anti-Bot Project “Cyber Clean Center (CCC)” was founded in December 2006 with the objective of reducing the number of bot-infected PCs to as close to zero as possible. It is the first attempt in Japan and one of few examples in the world to promote anti-bot measures, and is based upon collaboration between MIC, METI, security organizations, and several companies.

This project has eliminated bots and prevented reinfection by coordinating with ISPs and anti-virus vendors in notifying the users of many bot-infected PCs. Through these activities, the number of notified users has declined. The bot infection rate of broadband users in Japan was 2.0% to 2.5% in 2005, which had been reduced to as low as 1% in 2008. Activities have covered various media, which has enhanced the recognition of anti-bot measures and drawn attention from anti-bot organizations both inside and outside Japan. These facts indicate that activities have yielded results and their significance has been widely recognized.

However, there remain certain issues. One such issue is that the users of bot-infected PC have still not sufficient implemented security measures and there are also many users who are unwilling to take measures even if they have received several notifications. We must reach these users. Through our activities, we found the users of bot-infected PCs, notified them, and provided specific measures. However, it is the PC users who must actually institute anti-bot measures. Therefore, practical activities for raising the awareness of individual PC users are indispensable.

Another remaining issue is that bot infection spreads not just within Japan but from overseas. To eliminate bot-infected PCs from other countries, it is necessary to establish international collaboration against infections from overseas. From this viewpoint, it is necessary to publish the successful experiences of the CCC overseas.

We intend to build a system for international coordination by exploiting our know-how and expanding our continuing anti-bot activities.

Bibliography

[1] 高橋正和、他. フィールド調査によるボットネットの挙動解析. 情報処理学会論文誌 (Masakazu Takahashi et al, “Analysis of Bot Net Behavior Based on a Field Survey” (IPSJ Research Journal))
2006, Vol.47, No.8, p. 2512-2523.

[2] 有村浩一. ボット対策プロジェクト「サイバークリーンセンター」からみた国内のマルウェア対策 (Koichi Arimura, “Anti-Malware Measures in Japan Seen from the Anti-Bot Project “Cyber Clean Center””)
情報処理 (Information Processing), 2010, Vol.51, No.3, p.275-283

[3]中津留勇、他. マルウェア検出情報ログの分析による対策の検討 (Yu Nakatsuru et al, “Considering Countermeasures by Analyzing Malware Detection Log”)
Research Report, Computer Security, IPSJ, 2010, Vol.2010-CSEC-49, No.2

[4] “IT Keys - 先導的 IT スペシャリスト育成推進プログラム (“IT Keys – IT Specialist Program to Promote Key Engineers as Security Specialists”
http://it-keys.naist.jp/ (Reference 2010-08-20)

[5] “マルウェア対策研究人材育成ワークショップ (“Malware Specialist Fostering Workshop”)
http://www.iwsec.org/mws/2010/ (Reference 2010-08-20)

[6] “Microsoft Security Intelligence Report volume 8 (July – December 2009).”
http://www.microsoft.com/downloads/details.aspx?FamilyID=2c4938a0-4d64-4c65-b951-754f4d1af0b5, (accessed 2010-08-20).

[7] “ボットネット概要.” JPCERT/CC. 2007-04 (“Bot Net Summary” (JPCERT/CC, 2007-04)
http://www.jpcert.or.jp/research/2006/Botnet_summary_0720.pdf (Reference 2010-08-20)

[8] 小松文子、他：情報セキュリティ対策は社会的ジレンマか？ －ボットネット対策への適用－ (Ayako Komatsu et al, “Do Information Security Measures Mean a Social Dilemma? – Application to Anti-Bot Measures –)
Research Report, Computer Security, IPSJ, 2009, Vol.2009-CSEC-46, No.41