FY 2007

Cyber Clean Center (CCC) Activity Report

Anti-Bot Measures Project

Cyber Clean Center

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

Table of Contents

1 Introduction

Recently, various pieces of malicious software, known as Malware, have been causing increasing damage to Internet users.

Malware is a coined word from the prefix "mal", meaning "bad", and "software," and is now a generic term for software designed to cause damage, such as intrusions, attacks, etc., on users' PCs, and so forth. Malware includes various viruses, such as those in its strict sense, Trojan horses, worms, and BOTs[1]. BOTs, in particular, can break into an individual user's PC and remotely control it, and thereby make the PC take actions such as sending spam mails, engineering phishing or DDoS attacks to a desired target, and enable the theft of information from it. A network that is infected with a BOT and remotely controlled is called a "botnet," and forms a hotbed for cyber crime.

Given this situation, security measures are becoming more important with each passing day. Currently, however, security measures are often left to individual users. Many users, especially novices without sufficient knowledge of security, become infected with a BOT, a trend that is increasing. Security vendors in the private sector collect samples of Malware themselves and provide individual pattern files and antivirus software, but instances of Malware that cannot be detected even by the latest pattern files are increasing. Numerous variations of Malware are being generated in large numbers, and local infection cases are spreading, which indicates a situation where single security vendors alone cannot address every instance of

[1] It might be named BOT programs and BOT viruses.

Malware. MIC and METI jointly launched the "Anti-Bot Measures Project" in December 2006 to improve this situation. In the project, they have taken actions with an aim to reduce the threats from BOTs by promoting alert activities for BOT-infected users in close cooperation with ISP operators and security vendors. They are also steering the "Cyber Clean Center (CCC)" (https://www.ccc.go.jp/) as the project's portal site.

This document presents the FY 2007 Activity Report from the activities of three groups that are running CCC: the BOT Countermeasure System Operation Group, the BOT Program Analysis Group, and the BOT Infection Prevention Promotion Group.

1.1 What Is a BOT?

A BOT is a malicious program created with the aim of misusing personal computers and transmit infections, mainly through networks. The name "BOT" is derived from the fact that the way that infected machines resemble robots controlled by a malicious commander, known as a "Herder,".

Once a user's PC is infected with a BOT, a Herder can remotely control the PC through the Internet and make the computer take various actions, such as spying activities to steal information, nuisances such as delivery of spam mail, and attacks on a specific Web site.

Some BOTs have the ability to send the history of keyboard operations and information saved on a computer to the outside. It has been reported that these functions have caused instances of information leakage from PCs to the outside, such as attackers stealing credit card numbers, IDs, passwords, etc. and collecting addresses registered in the address books used for mail software. PC performance

may deteriorate because a system file has been tampered with, or the CPU has been overloaded when the PC is misused for purposes such as sending spam mail. Eventually, in the worst cases, users may be forced to reinstall the OS.

1.2 Current Status of Botnet

A botnet consists of tens of thousands or even millions of PCs infected with BOTs, forming a vast network controlled by a commander, called a Herder, via a C&C (Command & Control) server. BOT-infected PCs are manipulated with commands issued by the Herder and pose a great threat because they are misused for various purposes, for example, sending a large volume of spam mail for phishing, etc. and DDoS (Distributed Denial of Service) attacks on a specific site. Users who are using BOT-infected PCs are victims and at the same time unknowning victimizers, unaware that they are being used as a steppingstone to cyber crimes.

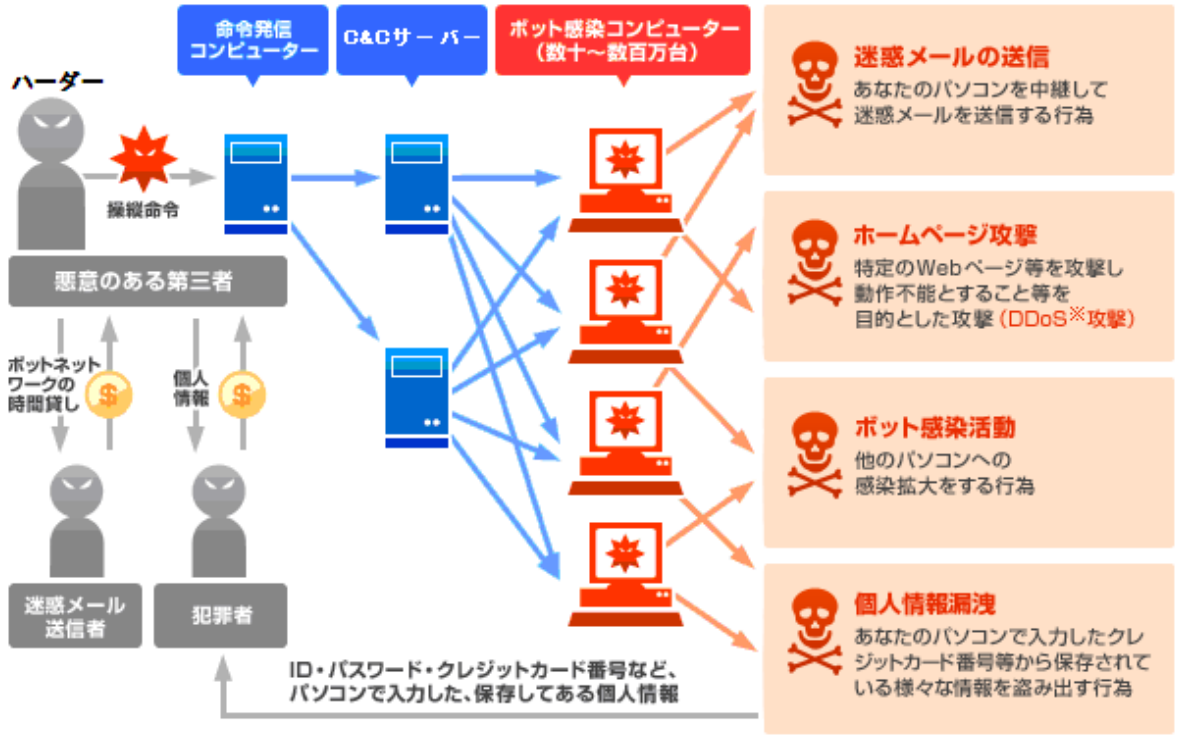


Figure 1-1: Threats from a Botnet

Surveys conducted in 2005 by organizations such as Telecom-ISAC Japan and JPCERT Coordination Center estimated that 400,000 to 500,000 PCs had been infected with BOTs, creating botnets, and approximately 80 percent of the current, malicious programs that are traveling over the Internet are regarded as BOTs. It has been reported that a PC that is not protected with security measures to become infected with a BOT in about four minutes when connected to the Internet.

Such damage caused by botnets is being incurred all over the world. Governmental sites, banks, etc. in the Republic of Estonia were hit by several large scale DDoS attacks in May 2007, and it has been reported that these attacks were waged using botnets. Many such DDoS attacks caused by botnets have been reported since Microsoft site was attacked in 2003.

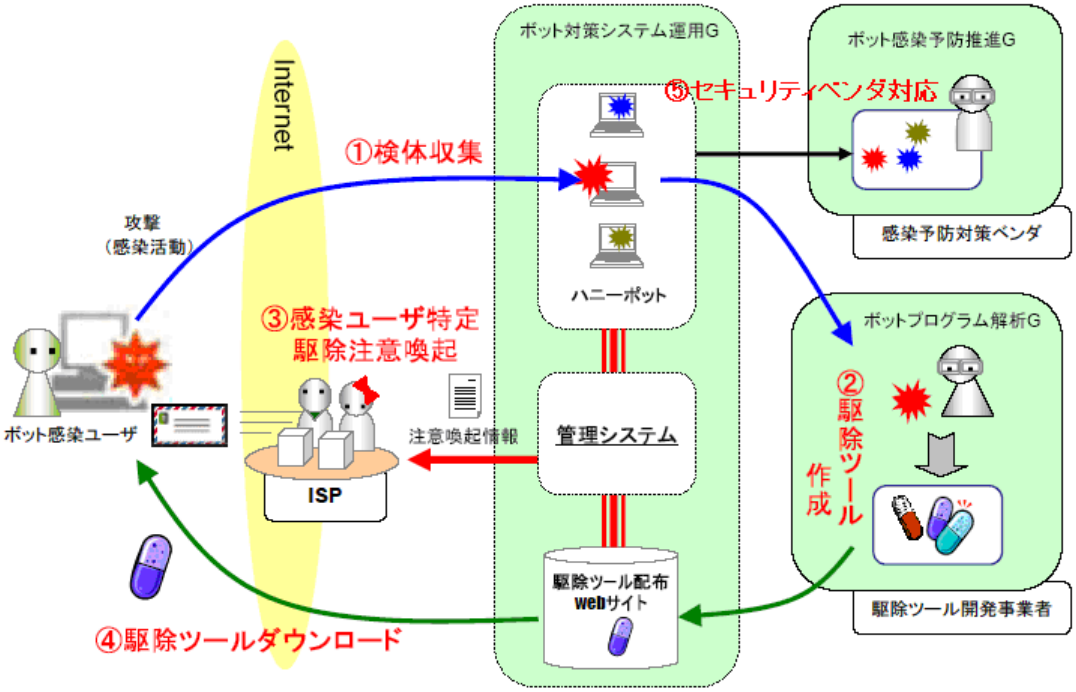
In New Zealand, a man who built a botnet consisting of one million or more PCs was arrested in November 2007. In Quebec, Canada, a person was also arrested on

the allegation of causing 45 million dollars' worth of damage by operating and illegally accessing a botnet consisting of about one million PCs.

In addition, the methods used to spread BOTs are constantly changing. This is demonstrated by an incident in March 2008 whereby a famous domestic site was altered in a way that it would deliver viruses such as BOTs to visitors. New types and variations of BOTs are detected every day, and we could believe that this is caused by the fact that BOTs are frequently upgraded using a self-maintaining function and that it is easy to add new patterns and functions to existing BOTs because their source code is available.

1.3 Overview of the Cyber Clean Center (CCC)

CCC is promoting alerts for BOT-infected users through activities illustrated in Figure 1-2 in cooperation with the Project Participating ISPs and others, such as security vendors, to minimize as far as possible the damage caused by infection of BOTs described above.



(1) Collecting samples	Collects samples of BOTs by detecting attack events (infection activities) from BOT-infected PCs with "decoy PCs" (honeypots).
(2) Developing disinfection tools	Analyzes BOT samples and develops "disinfection tools."
(3) Identifying infected users and alerting them to cleanse viruses	Identifies a source from which BOT attacks are waged in cooperation with ISPs and sends a BOT cleaning alert mail to the source.
(4) Downloading a disinfection tool	After an infected user reads the BOT cleaning alert mail, he can download and apply the disinfection tool from the CCC BOT countermeasure page by following the mail to get rid of the BOT.

(5) Supporting security vendors	Provides the collected samples of BOTs to security vendors. The security vendors incorporate the new samples into the pattern files in their antivirus software.

Figure 1-2: Overview of CCC Activity

CCC consists of three groups based on the nature of the work involved, performing its tasks under the Cyber Clean Center Steering Committee (CCC-SC).

Figure 1-3: Chart of CCC Operational Structure

BOT Countermeasure System Operation Group (Telecom-ISAC Japan)

This group operates the backbone system of this project, including honeypots and

alerts BOT-infected users to disinfect the virus through the Project Participating ISPs. The group also investigates the latest trends in BOTs.

Project participating ISPs as of the end of March 2008

IIJ, BIGLOBE, OCN, au one net, @nifty, hi-ho, ODN, Yahoo!BB, Internet MAGMA, IC-NET, GAONET, tigers-net.com, BaycomNet, bai Service, ASAHI Net, @NetHome, Cilas.net, BROADSTAR, isao.net, ZOOT, ipc-Tokai Internet Service, VECTANT, PIKARA, NETWAVE, WAKWAK, SANNET, mopera/mopera U, InfoSphere, TikiTiki Internet, MEGA EGG, Urban Internet, LCV-Net, LCNet, ZAQ, KATCH Cable Internet Service, KCN-Net, SYNAPSE, KCN Internet Service, Gunma Internet, ROSENET, MediaCat, K-Opticom eo, KIP-Internet, CATVY Internet, CanbleOne Cable Internet, TOKAI Network Club, JWAY Cable Internet, SCN Network Service, DAC System, Sendai CAT-V NET, Takaoka Cable Network, Commuf@, e-mansion, TAM Internet Service, Net3 Internet, aikis, avis, TCN Cable NET, CORALNET, TSTnet, DTI, NCM Cable Internet Service, N-plus, NOETSU Net, ParkNet, @hanno, Aitainet, FAMILYNET JAPAN CYBERHOME, VRTC Net, Web Shizuoka, Infovalley, FUSION GOL, Plala, Love Net, Mirai Net, Mediatti NET, and C-able Internet

BOT Program Analysis Group (JPCERT Coordination Center)

This group analyzes the features and techniques of the collected samples of BOTs and develops disinfection tools.

The group also conducts studies on effective analysis systems and develops countermeasure techniques in cooperation with the disinfection tool developer.

Disinfection tool developing business bodies

Trend Micro Incorporated

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

This group promotes the prevention of BOT infection by taking final charge of the BOT samples collected through CCC and by providing the samples to the Project Participating Security Vendors in an appropriate manner for incorporation into the pattern files of the vendors' antivirus software.

Project Participating Security Vendors

AhnLab Incorporated, Kaspersky Labs Japan Limited, Symantec Corporation, Sourcenext Corporation, Trend Micro Incorporated, Microsoft Corporation, and McAfee Incorporated

2 Activity Report - BOT Countermeasure System Operation Group

2.1 Overview

The BOT Countermeasure System Operation Group collects and analyzes the samples of BOTs and promotes alert activities, aiming to eliminate BOT-infected PCs.

In the sample collection and analysis phase, the group detects attacking events (infection activities) from BOT-infected users and collects BOT samples. It passes the collected samples to the BOT Program Analysis Group and asks the group to develop disinfection tools.

In the alert promotion phase, the group receives the newly-developed disinfection tool, identifies infected users in cooperation with the ISPs, and sends alert mails to them. When the users receive the mails, they download the disinfection tool through the BOT countermeasures site. The group also distributes the disinfection tools to general users through the official CCC site.

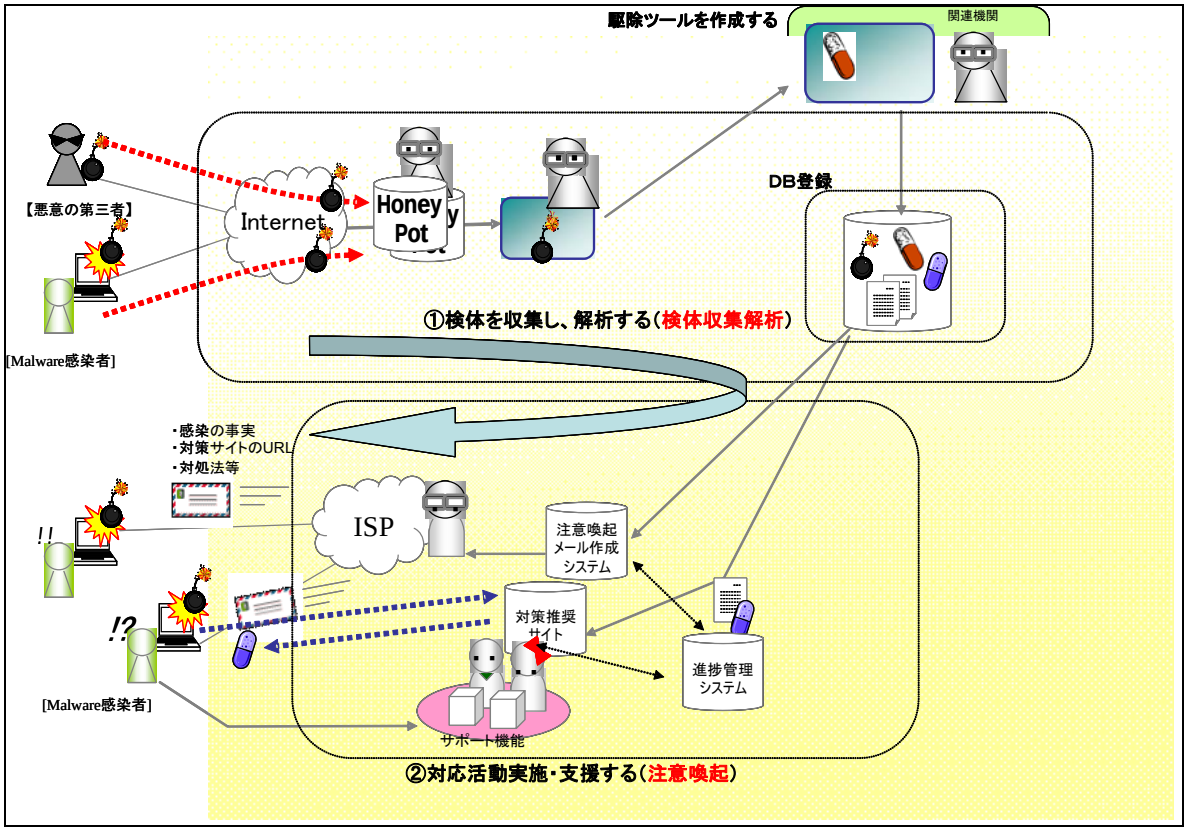


Figure 2-1: Overall View of BOT Countermeasure System Operation Group

2.1.1 Sample collection and analysis

This group detects attacking events (infection activities) from BOT-infected users and collects the samples of BOTs as a trigger to alert users. While various types of methods are used to spread BOTs, most of them target the vulnerabilities of a PC's OS. For this reason, it is possible to observe infection activities of BOTs and identify infected PCs (users) with the ISPs by installing decoy terminals (honeypots) on which OS vulnerabilities are deliberately left open. Disinfection tools can be developed by collecting the samples of many BOTs through these honeypots. The collected samples of BOTs include duplicates and those that have already been addressed by antivirus software. The task to identify the unique types of samples is called

"identification analysis" and those that have been analyzed using this method are called "identified, unique samples." The group performs the task of scanning the identified, unique samples with antivirus software (using the latest patterns used by Trend Micro for scanning BOTs) and excluding those that have been addressed by antivirus software (this task is termed "known and unknown isolation analysis"). After this task, the BOT Program Analysis Group develops disinfection tools for the samples that have not been addressed (the unknown samples).

2.1.2 Alert activity

The BOT Countermeasure System Operation Group analyzes communications to and from the BOT samples collected with the honeypots and identifies the ISP(s) used by the infected users, passing the infected user information to the ISP(s). Then, the alert activities are performed in the following way: the ISP sends mails to the infected users, indicating that they have been infected with a BOT and alerting them to disinfect the virus. The following describes the process:

(1) The group identifies the ISPs used by infected users with information on the attacking events (infection activities) collected by the sample collection and analysis system.

(2) If the identified ISPs belong to the Project Participating ISPs, the ISPs are asked to identify the infected users and alert them. (The group identified infected users in cooperation with 8 ISPs in FY 2006 and increased the number to 68 ISPs in FY 2007 to improve the coverage rate of ISPs in Japan.)

(3) The ISPs identify the infected users and alert them that they may be affected with a BOT by e-mail, for example.

2.2 Status of Activity and Achievements

This project discloses the results of the alert activities on a monthly basis to the public in the form shown in Figure 2-2, through the CCC official site (https://www.ccc.go.jp/).

The results include information on the output from collecting and analyzing samples ((1) to (7) in the figure) and the number of disinfection tool downloads from the public opening site.

As of March 2008, the project has collected a total of 7,673,279 samples and the identified, unique samples amount to 215,338 types. Among them, 10,082 samples that could not be detected with commercially available antivirus software at the time of collecting them were identified. Regarding the alert activities, 232,487 e-mails were sent to 54,703 persons, and about 29 percent of the infected users downloaded disinfection tools and followed the countermeasures.

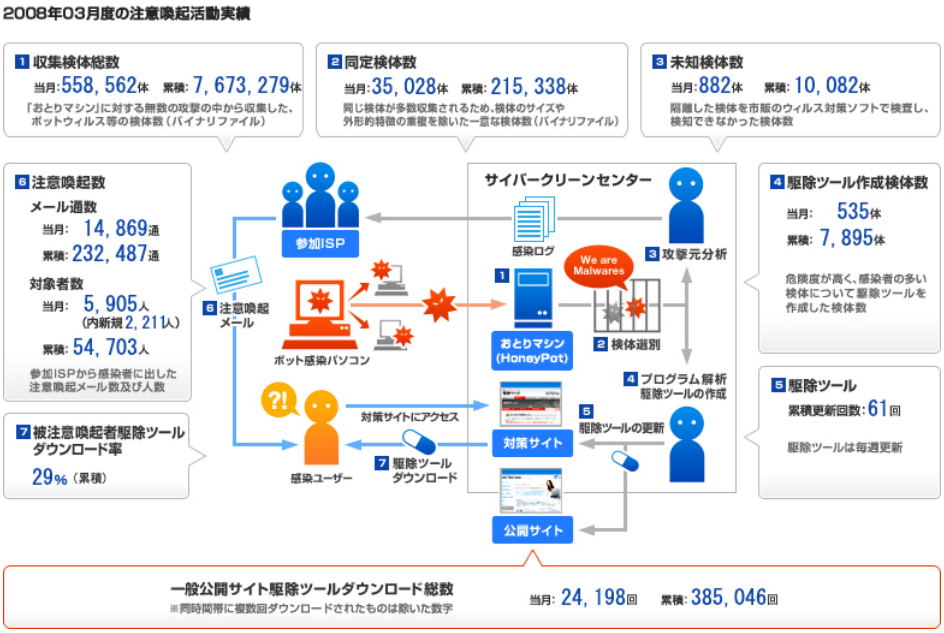


Figure 2-2: Activity Result - Cumulative Total of Actual Results from February 2007 to March 2008

2.2.1 Sample collection and analysis

To alert BOT-affected users, it is necessary to capture infection and attacking activities adopted by BOTs and collect and analyze the samples of the BOTs to develop disinfection tools.

This section shows the status of sample collection and analysis activities from April 2007 to March 2008.

(1) Changes in number of collected samples

The sample collection and analysis system lures BOTs into a system called a honeypot through network lines and collects them as BOT samples.

The monthly number of collected samples is approximately 540,000 (or approximately 18,000 on a daily basis). The collected samples at this point in time include the duplicate and/or known samples.

Figure 2-3 shows the changes in the number of collected samples by month.

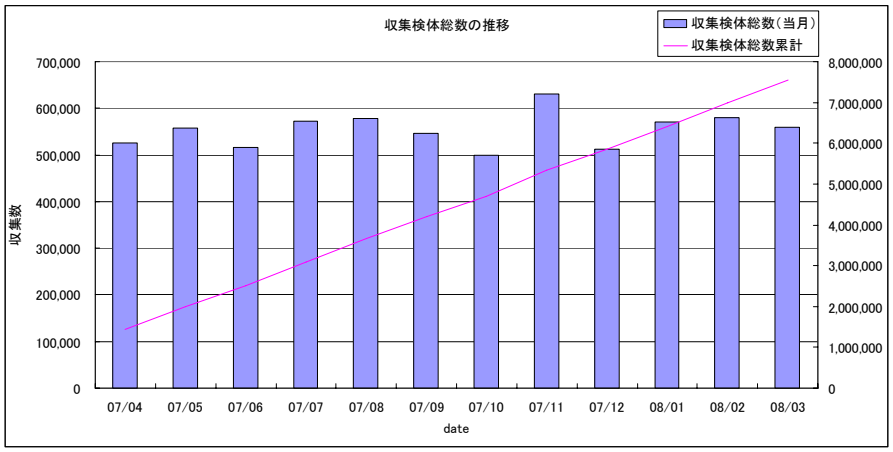


Figure 2-3: Changes in Total Number of Collected Samples

(2) Changes in the number of identified, unique samples

The monthly average of the numbers of identified, unique samples derived from identifying and analyzing the collected samples is approximately 15,000, which amounts to approximately 500 samples on a daily basis.

Figure 2-4 shows the change in the number of identified, unique samples by month. The figure shows a decline in October and November 2007, which is because some types of BOTs delivered from a specific overseas site decreased during that period. In February 2008, as file infection type viruses that infected executable files within the honeypots grew, the number of BOT types increased. Particularly, the samples that repeatedly grew in large numbers were “explosion”- type BOTs, which can wage many attacks. This type of BOT showed an increasing trend after February.

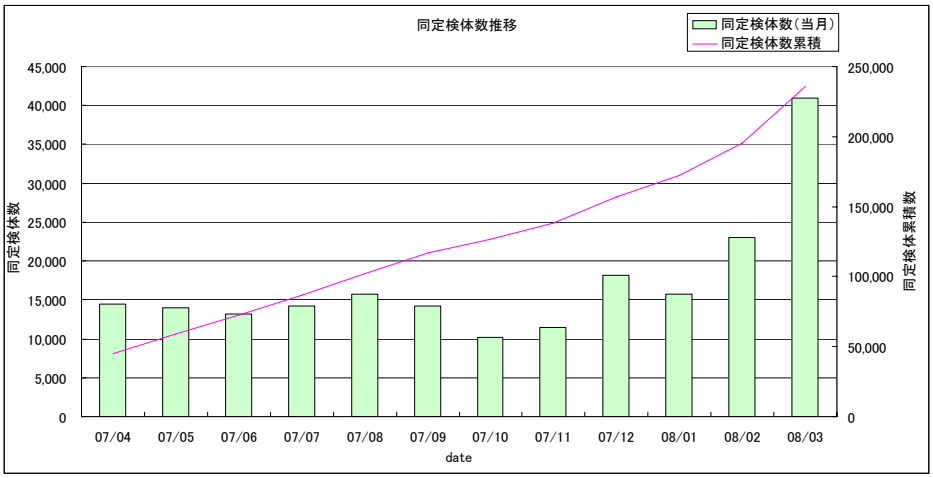


Figure 2-4: Changes in Number of Identified, Unique Samples

(3) Changes in the identified, unique samples, known and unknown

From the statistics of results from performing the known and unknown isolation analysis on the identified, unique samples (analyzing whether they can be addressed with commercially available antivirus software), the analysis

determined that known samples totaled 14,000 and those unknown totaled 1,000 (approximately 7%) among an average of approximately 15,000 identified, unique samples per month. This means that approximately 30 unknown samples were collected on a daily basis.

Figure 2-5 shows the changes in the number of known and unknown identified, unique samples by month. The figure indicates that the number of unknown identified, unique samples fluctuates each month and the ratio of the samples to the number of identified, unique samples decreases. Looking at the slope of the cumulative total of the unknown identified, unique samples (indicated by the line graph), it appears that an increasing number of samples had been on a declining trend, compared to that of the beginning of 2007, as shown by the slope becoming gradually more moderate.

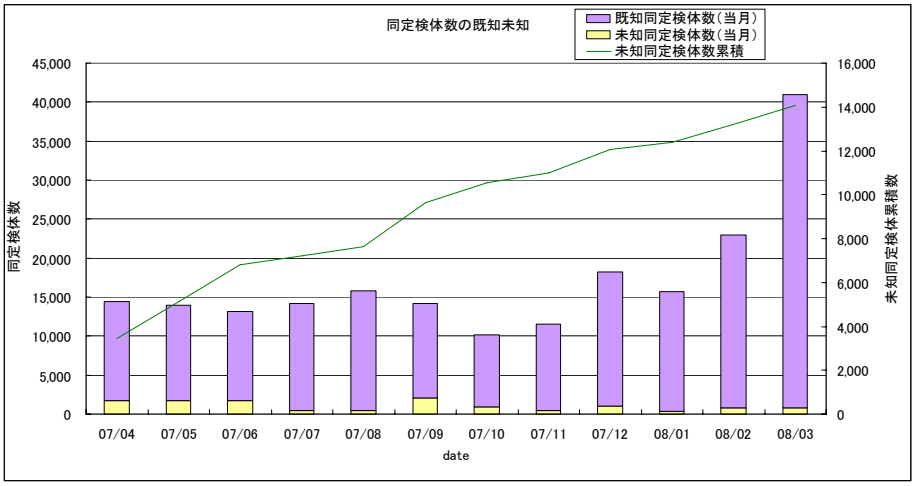


Figure 2-5: Changes in Number of Known and Unknown Identified, Unique Samples

The reason why the number of identified, unique samples was low although the number of the entire collected samples appears high in November was because BOTs that waged many attacks ran rampant in October and November. Figure 2-6 shows how BOTs ran rampant within the fiscal year.

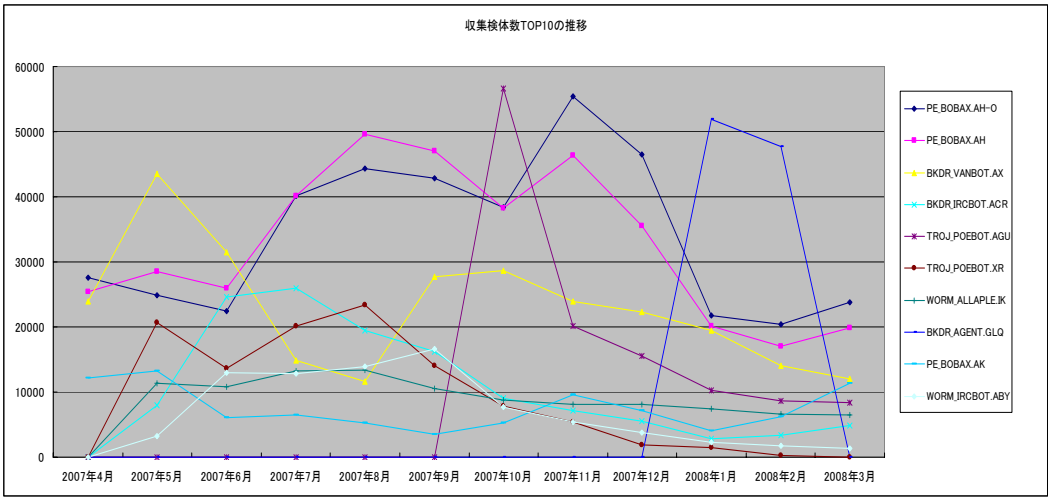


Figure 2-6: Changes in Samples with Top 10 Attacks among the Collected Samples

(4) BOT distribution sources

BOTs have been distributed not only from within Japan but also from overseas.

Figure 2-7 classifies the sources of distribution of collected samples (attack sources) into "From within Japan," "From overseas," and "Between infected honeypots" (internal infection), and shows the monthly change in the number of attacks. It indicates that the total number of attacks (the number of collected samples) slightly increased as the number of attacks from overseas increased, although the number of those from within Japan showed a slight declining trend.

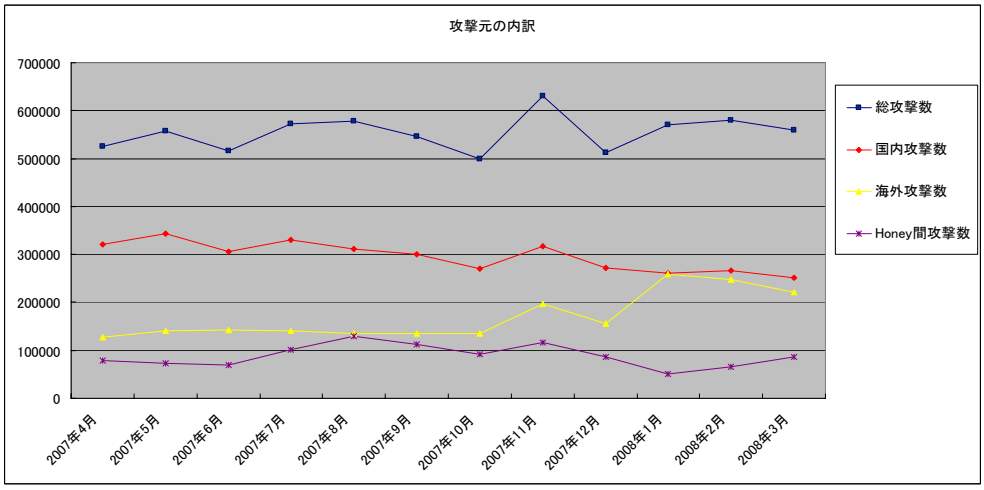


Figure 2-7: Breakdown of Attack Sources

Figure 2-8 shows the breakdown of the total number of attacks with the ratios of the attacks from within Japan, those from overseas, and those between the infected honeypots (internal infection) to the total number of attacks. This figure also shows that the rate of attacks from overseas increased and those from within Japan decreased.

The reason why the attacks from overseas increased is because attack activities became active from specific overseas sites.

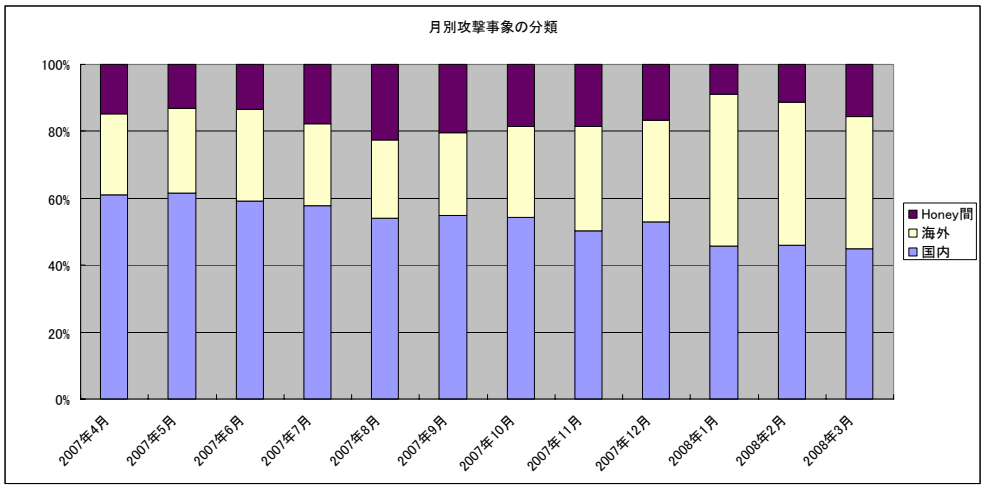


Figure 2-8: Ratios of Attack Sources

2.2.2 Alert activities

(1) Status of user measures performed

To eliminate BOT-infected PCs, it is vital to identify BOT-infected users and alert them to the fact. The BOT Countermeasure System Operation Group has been alerting infected users through e-mails in cooperation with the Project Participating ISPs.

In FY 2007, the number of alert e-mails sent was 232,487 and the number of alerted users was 54,703 (see Figure 2-2).

The alert mails in FY 2007 achieved the following: rate of visiting the countermeasures site was approximately 39%, rate of downloading disinfection tools was approximately 30%, and the Windows Update rate was approximately 27%. In addition, the rate of users' reporting that all the countermeasures had been completed was approximately 15% (see Figure 2-9).

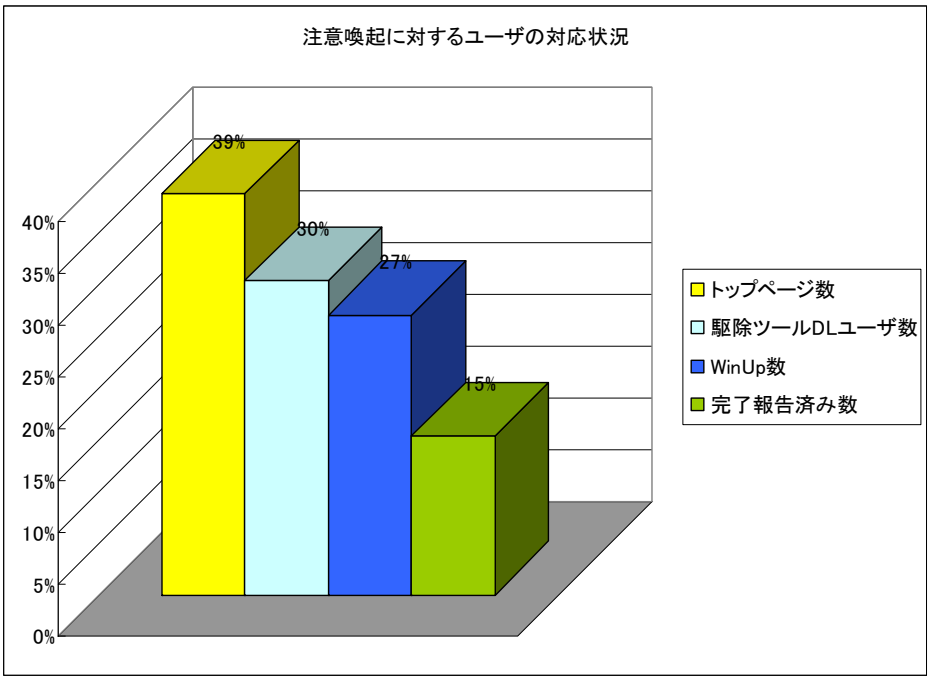


Figure 2-9: Status of Users' Responding to Alerts (April 2007 to March 2008)

(2) Status of user support

The Project Participating ISPs took charge of providing user support to the alerted users, but the BOT Countermeasure System Operation Group directly

supported some alerted users that had been escalated by the ISPs to the group. These user support activities shed light on several issues as follows:

① Cases where Windows Update could not be performed

- The altered hosts file prevented users from connecting to the Windows Update site
- As one file infection type virus (particularly, VIRUT) became more rampant, a system file was infected in the course of Windows Update
- When LANdriver was optimized in Windows XP SP2, Web connection timed out as the resources for PC and lines were consumed

② Cases where a broadband router was not installed

- Approximately 90 percent of users to whom the BOT Countermeasure System Operation Group provided direct support were infected through attacks that homed in on OS vulnerabilities because users did not install broadband routers

③ Cases where users misunderstood their antivirus software

- Many users continued to use their preinstalled antivirus software in their PCs without updating its pattern files since purchasing it
- Some users mistook a personal firewall function for antivirus software (When some users were using a personal firewall in conjunction with antivirus software and unauthorized access was made to their system, they had a false idea that the antivirus software was functioning properly because the personal firewall issued a warning even if the patterns in the

software were not updated (their security measures looked as if they had been working because a warning message was issued although BOTs could not be disinfected because the patterns in the antivirus software were out-of-date))

- Some users thought that the email virus detection service provided by their ISP was sufficient to protect their systems (an email virus detection service alone cannot deal with BOTs that transmit infections, target vulnerabilities or when users were simply accessing the Internet)

CCC introduced Windows Update as one of the basic measures against BOTs, but in reality many users were infected with BOTs because they did not perform Windows Update. When CCC asked these users to perform Windows Update, there were many cases where Windows Update could not be performed due to BOT infection.

The installation of a broadband router is a very effective measure for BOTs that transmit infections targeting vulnerabilities. CCC realized, however, that even users with comparatively high awareness of security did not fully recognize the effectiveness of broadband routers.

CCC learned that there were various misunderstandings concerning antivirus software and some cases where users uninstalled antivirus software because their systems got slower or due to other reasons even though they had installed it themselves at an earlier date.

(3) Approaches towards improving the effectiveness of BOT countermeasures

The BOT Countermeasure System Operation Group has been performing various improvements towards enhancing the effectiveness of BOT countermeasures. One of these is to improve the countermeasures site that the infected users access. This site provides various pieces of information on BOT countermeasures, including the distribution of disinfection tools, but at first the site included many pages before users reached the desired countermeasure steps. For this reason, many users terminated the countermeasure steps before completing the final important stages. Consequently, the group reviewed the structure of the pages in the site, and improved it to provide all the BOT countermeasures in one page.

At first, it also explained to users that they should perform Windows Update after a disinfection tool. But, even if users could get rid of BOTs with a disinfection tool, there were many cases where they were infected again with a BOT during the Windows Update process due to Windows OS vulnerabilities. For this reason, the group reviewed the step so that users should perform disinfection again after the Windows Update process had been completed.

In addition, it improved the countermeasures site whenever the necessity arose, such as formulating the necessary steps to install a broadband router.

As another major approach adopted by the group, some Project Participating ISPs started alerting users through postal mail as well as e-mails as an alert channel. As the existing alert e-mail method failed to have some users take measures against BOTs because they did not read the alert e-mails, CCC sent additional postal alert mails, which improved the access rate to the

countermeasures site from approximately 30% when alerts were only e-mailed to approximately 50%.

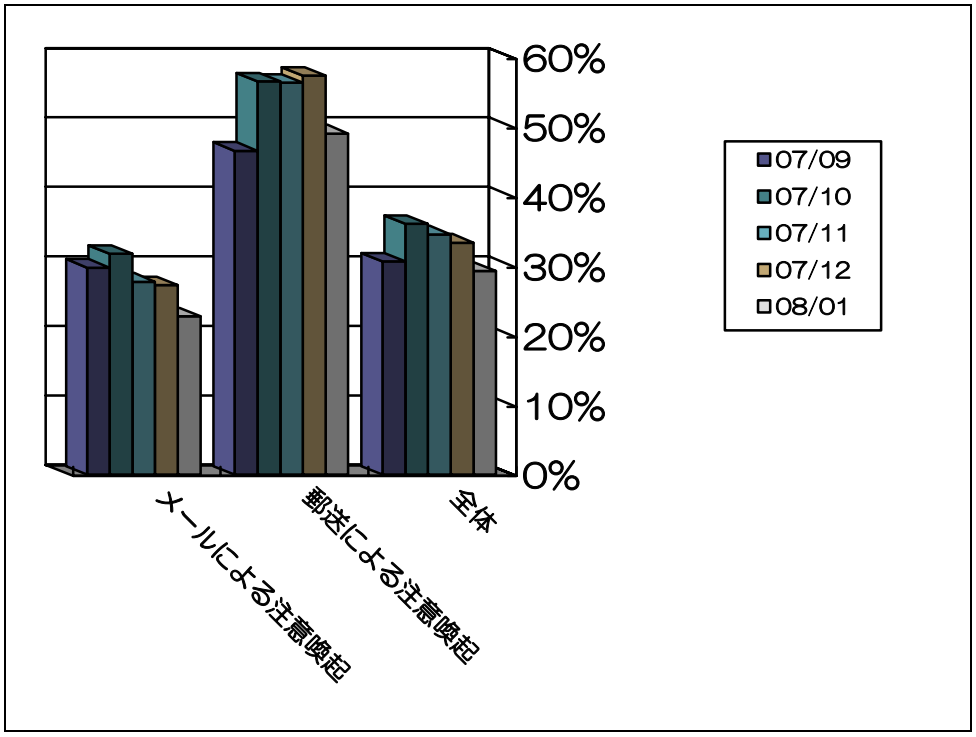


Figure 2-10: Effectiveness of Postal Alert Mail by an ISP

(4) New approaches

The group adopted new approaches to make more people in Japan aware of the Anti-BOT Measures Project in FY 2007.

The first approach was to increase the number of the Project Participating ISPs. In the beginning of FY 2007, the group performed alert activities in cooperation with 8 ISPs, but to expand the scope of users to be alerted, enhance cooperation with ISPs, and promote awareness activities intended for users, it extended contact to a wide range of ISPs in Japan and expanded the Project Participating ISPs to 68 ISPs, as of the end of FY 2007. Note that CCC

determined that ISPs could participate in the Anti-BOT Measures Project in the following two modes: (1) where an ISP identifies and alerts infected users by directly connecting to the system on the side of CCC, based on information such as the number of BOT-infected users in the ISP; and (2) where an ISP alerts BOT-infected users based on requests from CCC without preparing any special systems.

The second approach was to open the BOT Disinfection Activity Declaration site (http://botkujo.jp/).

The BOT Disinfection Activity Declaration site was intended to disseminate awareness of BOT countermeasure activities by communicating information about the threats from BOTs to the general public in plain terms, and introducing comments and other information from persons responsible for this project at Project Participating ISPs. The group asked the Project Participating ISPs to set up a link to the BOT Disinfection Activity Declaration site whereby users could be guided from the site to the CCC official site when they needed actual BOT countermeasures.

Figure 2-11: BOT Disinfection Activity Declaration Site (http://BOTkujo.jp/)

In addition, the group has made every possible effort to spread information about BOT countermeasures and make users aware of them through activities such as preparing leaflets that communicate the threats and countermeasures of BOTs in plain terms and disclosing the results of monthly CCC activities to the public (https://www.ccc.go.jp/).

Figure 2-12: Leaflets

2.3 Future Development

The practical approach adopted by this project is producing results. For example, the number of infected users has started to decrease in some of the Project Participating ISPs through their activities. Awareness of the project has also been heightened, indicated by the fact that the number of access attempts to the CCC official site is increasing due to the media covering the work we are undertaking.

In FY 2008 just as in FY 2007, the group intends to aim to further decrease the number of BOT-infected PCs by continuing alert activities for BOT-affected users. For this reason, it will develop closer cooperative relations with Project Participating ISPs, and not only prompt as many users as possible to perform BOT countermeasures, but also vigorously promote better alert methods and so forth, such as further improvements to the countermeasures site. The group will perform awareness campaigns to prevent BOT infection using various channels in parallel with our alert activities.

3 Activity Report - BOT Program Analysis Group

3.1 Overview

The BOT Program Analysis Group analyzes the samples of BOTs collected with honeypots and develops disinfection tools. Note that the group performs in-depth analysis on the analyzed BOTs using static analysis technology whenever necessary.

3.2 Analysis

When analyzing the samples, the group performs the tasks described below.

3.2.1 Developing a disinfection tool

Regarding the samples that have not been addressed by commercially available antivirus software, the group investigates information such as the file types related to the infection of BOTs and develops disinfection tools.

(1) Creating a response list

The group creates a list of prioritized responses because quick actions must be taken against samples with severe impact.

- Obtain samples of BOTs and information related to them from the BOT Countermeasure System Operation Group.
- Extract samples to be analyzed based on specific criteria (priorities).

The criteria have been set as shown in Table 3-1:

Table 3-1: Criteria for Samples to Be Extracted

Criteria	Does Sample Attack?	How Antivirus Software Addresses Sample
1	Yes	Unknown by antivirus software from the disinfection tool developer and two other companies
2	Yes	Unknown by antivirus software from the disinfection tool developer (not considering whether antivirus software from two other companies has or has not known the sample)
3	No	Unknown by antivirus software from the disinfection tool developer and two other companies
4	No	Unknown by antivirus software from the disinfection tool developer (not considering whether antivirus software from two other companies has or has not known the sample)

● Create a table of responses about the samples that the group determined to reflect in the disinfection tool.

● Send the response list to the BOT Countermeasure System Operation Group.

(2) Developing a disinfection tool

Creating the response list described in (1) above is a daily task and developing a disinfection tool described in (2) is a weekly task.

- For the samples that have been collected by Monday, the group analyzes them and develops a disinfection tool(s) for them by the following Wednesday each week.
- Provide the developed disinfection tool(s) to the BOT Countermeasure System Operation Group.
- The BOT Countermeasure System Operation Group distributes the disinfection tool(s) through the countermeasures site accessed by the BOT-infected users who were alerted. It also provides the tool(s) to general users through the CCC site.
- ISPs e-mail a request to disinfect the BOTs to the BOT-infected users.

3.2.2 Performing detailed analysis

As a result of the analysis described above, the group performs in-depth analysis on the following items for the samples of a BOT whose current status must be determined or which is highly dangerous to users. The group performs this process on an as-needed basis.

- Behavior pattern of BOTs per se
- Technologies used to generate BOTs
- Infection routine of BOTs

3.2.3 Providing samples to the BOT Infection Prevention Promotion Group

The group passes the samples provided by the BOT Countermeasure System

Operation Group and information related to them to the BOT Infection Prevention Promotion Group.

Samples received from the BOT Countermeasure System Operation Group are provided to the BOT Infection Prevention Promotion Group on the morning of the following business day. This procedure was updated so that the samples could be provided more quickly to the BOT Infection Prevention Promotion Group and consequently security vendors could more quickly deal with the samples collected in this project.

This change enabled the group to provide the samples received from the BOT Countermeasure System Operation Group to the BOT Infection Prevention Promotion Group on the same day, which is one day earlier than before the group changed this procedure. As a result, the following data provided by the BOT Infection Prevention Promotion Group reveals that the updated procedure contributes to circulating pattern files for BOTs to users more quickly than before (Table 3-2)

Table 3-2: Samples Reflected in Pattern Files after Being Provided

	For 20 Days before Change	For 20 Days after Change
Samples already reflected when obtained	97.0%	90.5%
Samples not reflected when obtained	3.0%	9.5%

3.3 Enhancing the functions of disinfection tools

The group has enhanced the functions of disinfection tools to improve them from the viewpoint of users. The enhancements are as follows:

3.3.1 Adding a validity period setting function (released April 2007)

If users do not use the latest disinfection tool and continue to use an out-of-date tool, they cannot deal with new and variant BOTs. Although they are infected, they may have a false idea that "I am not infected" or "we are safe because we have taken measures against BOTs," because their out-of-date tools do not detect any BOTs. For this reason, the group has added a function that enables users to set up a validity period for their disinfection tools so that they cannot continue to use disinfection tools with out-of-date pattern files.

3.3.2 Adding standard setting mode based on sample types (released April 2007)

BOTs can be divided into two types: one type of virus continues to function as a resident processes in PC memory, and the other transmits infection to PC resources and exists as files. As it takes some time for disinfection tools to search PC resources for the infected file, the search option was originally set to memory search as a standard setting (by default).

However, as the group was required to provide disinfection tools appropriate to each type of BOT, based on the features of BOTs that transmitted infections to users that would receive BOT cleaning alerts, it added a standard setting mode whereby

users could select which area is to be searched (memory or hard disk).

After that, as file infection type (hereinafter, "PE type") BOTs soared, it provided disinfection tools for which both memory search and file search were defined as the standard setting. Table 3-3 shows this change to the disinfection tool standard setting:

Table 3-4: Change of Disinfection Tool Standard Setting

Site	Mode Setting before April 2007	Mode Setting when Released in April 2007	Mode Setting after November 2007
Counter-measures Site for Infected Users	Only memory search was configured as the standard setting	Either memory search or file search was configured as the standard setting, based on the samples that had transmitted infection to users who were alerted to cleanse them	Both memory search and file search are configured as the standard setting
General Site	Only memory search was configured as the standard setting	Both memory search and file search were configured as the standard setting	Both memory search and file search are configured as the standard setting

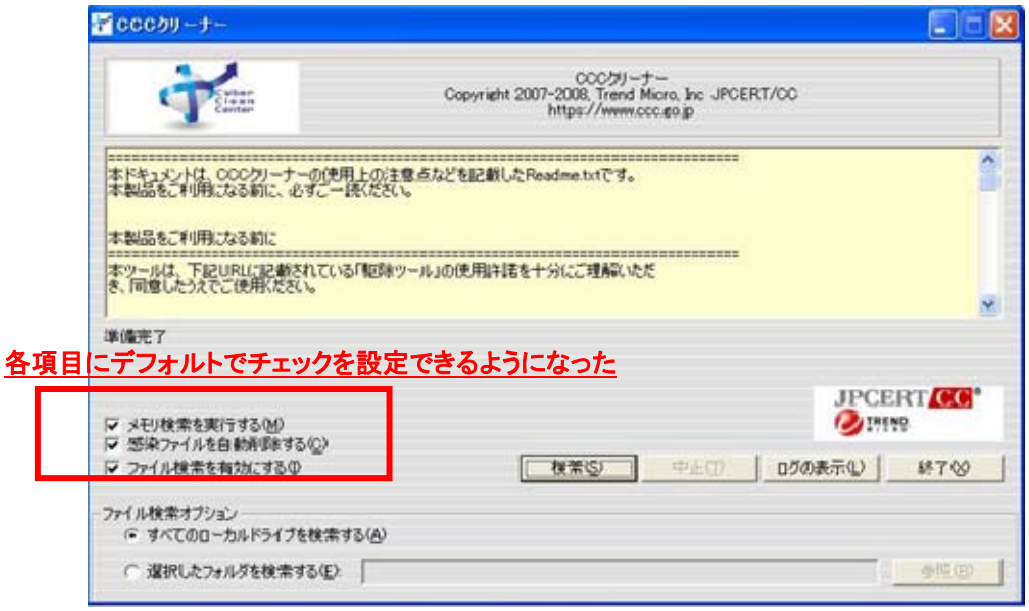


Figure 3-1: Window Incorporating the Standard Setting Mode

3.3.3 Supporting Windows 98/Me

In FY 2007, the group received a request from users, saying "we wish you to configure disinfection tools to support Windows 98/Me because antivirus software products supporting Windows 98/Me are becoming fewer." As the OS vendor, Microsoft, had already terminated support for Windows 98/Me, however, the group decided that its disinfection tools would not support these OSs. In addition, as a result of investing trends in security vendors, it turned out that support for antivirus software for Window 98/Me would be generally terminated around the end of 2008.

For this reason, the group asked the users to understand the risks involved in continuing to use Windows 98/Me because disinfection tools could not deal with new vulnerabilities for these OSs when they were found because the OS vendor had terminated support for the OSs and had stopped providing security updates.

The group also decided to introduce users who would inquire about Windows

98/Me support to an article posted by the media (http://www.itmedia.co.jp/enterprise/articles/0707/10/news005.html) or the article "Call for Attention in May 2007" (http://www.ipa.go.jp/security/txt/2007/05outline.html#5) on information security by INFORMATION-TECHNOLOGY PROMOTION AGENCY (IPA) as a tentative way to avoid problems, to be seen as a temporary measure until they upgraded their OS (including replacing PCs by new purchases).

3.3.4 Support for Windows Vista (released in November of FY 2007)

The group supported Windows Vista to prompt more users to use disinfection tools and promote the detection and disinfection of BOTs.

3.3.5 Detection status transmission function (released in November of FY 2007)

The group added a function to transmit information, such as the status of BOTs detected, to CCC after running a disinfection tool. The function was intended to implement more effective BOT countermeasures by taking advantage of the information sent in by users.

The information gathered by this function includes the following. Note that users can choose whether or not they want to send information when starting to run the disinfection tool.

- Information on OS version
- Time and date executed
- Number of detections/number of removed BOTs/number of BOTs not

removed

- Name of detected malware
- Error information

3.4 Trends in BOTs

3.4.1 Trends in collected BOTs

Table 3-5 shows the top 15 families of BOTs after this project performed identification analysis on BOT samples in FY 2007. As shown in the table, the collected BOTs include a wide variety of types, including worms.

Table 3-5: Top 15 Families of Collected BOTs (FY 2007)

	BOT Family Name (Name of BOT Detected by Antivirus Software from Trend Micro Inc.)	Type	Number of Identified, Unique Samples
1	WORM_ALLAPLE	Worm type	86458
2	PE_VIRUT	PE type	65234
3	WORM_BOBAX	Worm type	10489
4	PE_BOBAX	PE type	6420
5	WORM_CHELI	Worm type	3061
6	PE_SALITY	PE type	2136
7	WORM_RBOT	Worm type	1360
8	PE_VBAC	PE type	1107
9	BKDR_VANBOT	BKDR	1042

		type	
10	WORM_SDBOT	Worm type	471
11	TROJ_AGENT	TROJ type	394
12	BKDR_IRCBOT	BKDR type	350
13	TROJ_QHOST	TROJ type	337
14	BKDR_POEBOT	BKDR type	299
15	WORM_IRCBOT	Worm type	279

Table 3-6 summarizes the definition of each BOT type according to Trend Micro Incorporated.

Table 3-6: Definitions and Types of BOTs

Type	Definition	URL
PE type	Takes the standard Windows executable file format "Portable Executable." The software detects file infection type viruses that transmit infections to PE format files (extensions are COM, EXE, SYS,	http://jp.trendmicro.com/jp/threat/glossary/p/pe/

	etc.) and indicates them by prefixing "PE" to them such as "PE_xxxxxx."	
Worm type	Malicious programs that aim to spread viruses to other PCs through networks are generally called worms.	http://jp.trendmicro.com/jp/threat/glossary/jp-wa/worm/index.html
TROJ type (Trojan horse type)	Generic name for malicious programs that do not transmit infection to other programs.	http://jp.trendmicro.com/jp/threat/glossary/jp-to/troi-no-mokuba/index.html
BKDR type (Backdoor type)	A TROJ type. Aims to manipulate PC of an infected user without restrictions and steal important information such as passwords.	http://jp.trendmicro.com/jp/threat/glossary/jp-ha/backdoor-gaata/

Many of the latest PE types include not only the file infection function but also other functions such as worms, backdoors, and downloads.

PE type BOTs have the ability to embed malicious code into the executable files of the OS or an application. However, in considering BOTs of types other than PE types, we need to be aware that the BOT per se is a program file. From these facts, the group could infer that attackers design BOTs in a way that they not only attempt to hide the BOTs they create in order to prevent detection, but also to make the viruses difficult to be detected and disinfected, based on the assumption that they will actually be found.

3.4.2 Soaring PE type BOTs

As the PE type BOTs transmit infections to files that exist in the OS or an application, even the same type of BOTs may spread the infection to different files. In that case, as the same BOT samples are counted as different ones, many cases of infection may be found on one PC.

If we look at the statistics (Figure 3-2) into which the group summarized the samples by family after having identified the unique samples collected by honeypots in this project, we can see that the PE_VIRUT family has been soaring since November 2007.

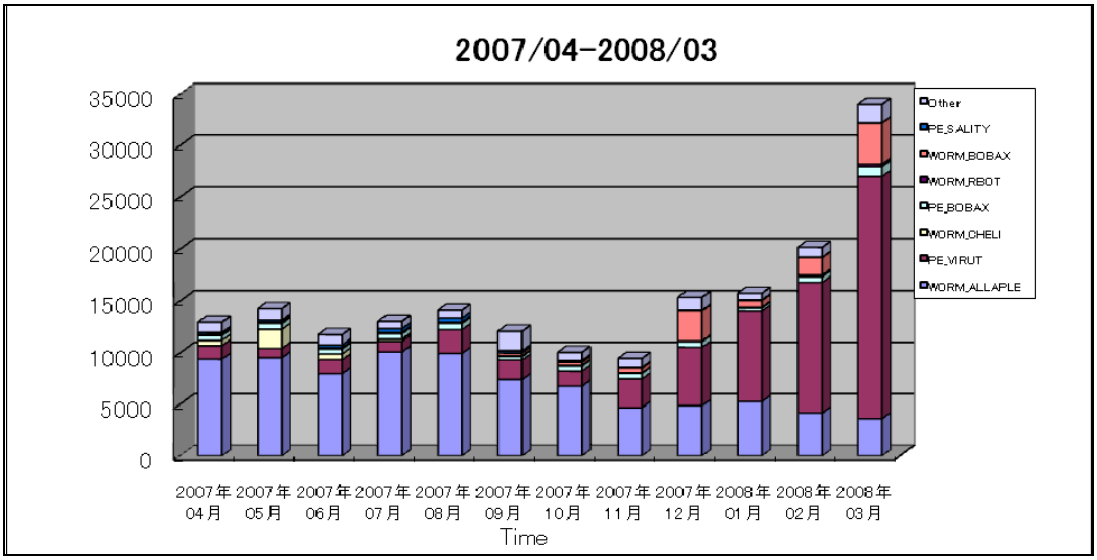


Figure 3-2: Comparison of Ratios of Collected BOT Families

The PE_VIRUT family is equipped with a backdoor function and has the ability to receive remote commands through an IRC channel after it connects to a C&C server once a user becomes infected.

3.4.3 PE type BOTs and considerations on disinfection tools when addressing them

In terms of infection method, the PE type BOTs can generally be categorized into the following types: those that insert a malicious code into the head or tail of the code in an original file; those that insert a malicious code into an unused section of an original file; and those that overwrite parts or all of the code in an original file.

At the same time, as disinfection tools function, sequentially searching the memory area or disk area on a PC, an infected file that has not been disinfected yet may perform infection activities on a file already identified and disinfected in the course of the search and disinfection process. In this case, although the results from the searching and disinfecting process in a disinfection tool indicate "all removed," it is likely that some viruses still remain.

If users are infected with a BOT belonging to the type that overwrites parts or all of the code in an original file with a malicious code, users cannot restore the original file because the program information for the file has been lost. If the original file is an executable file of the OS or an application, a recovery operation (initialization) may be required. If users are infected with PE type BOTs other than this type, they can disinfect the BOTs or prevent infection by such viruses by installing commercially available antivirus software, updating the pattern file, and configuring the software to always monitor the contents of the PC.

3.5 Future Developments

In FY 2007, the group adjusted the operation schedule and added additional functions to the disinfection tools, in addition to the current scheme (creating a

response list, sample analysis, and developing disinfection tools) in FY 2006.

In FY 2008, the group intends to maintain a stable supply of disinfection tools by continuing the operations of the current scheme, and also to deal with soaring PE type BOTs.

(1) Enhancing the functions of disinfection tools

The group will develop additional functions to display a warning when users are infected with PE type BOTs and to guide them to the countermeasures based on current disinfection tools.

(2) Developing disinfection tools

The group will maintain a stable supply of disinfection tools.

(3) Analyzing BOTs

The group will perform trend analysis on BOTs, etc. by using the accumulated results of dynamic analysis and static analysis.

(4) Assisting diffusion and awareness activities

The group will assist the diffusion and awareness activities of BOT infection countermeasures.

4 Activity Report - BOT Infection Prevention Promotion Group

4.1 Overview

The BOT Infection Prevention Promotion Group commits itself to this project in cooperation with security vendors (hereinafter, "Project Participating Security Vendors") to enhance BOT infection countermeasures and prevent the recurrence of damage caused by the same BOTs, for general users. Specifically, the group provides samples of the BOTs collected in this project to the Project Participating Security Vendors, enabling the vendors to reflect those samples in the pattern files in the antivirus software they are selling. This way, if users keep the pattern files for their antivirus software updated, the antivirus software can detect and disinfect the BOTs collected by the project. Consequently, security measures can continue to be improved.

4.2 Project Participating Security Vendors

The respective Project Participating Security Vendors are legal entities that performs strict administrative standards on the samples, set up departments to analyze them in Japan, and have a substantial past record of supplying their antivirus software and providing related services in Japan. The group is campaigning to promote the infection prevention in resources such as PCs for users with these infection countermeasure vendors participating in the project.

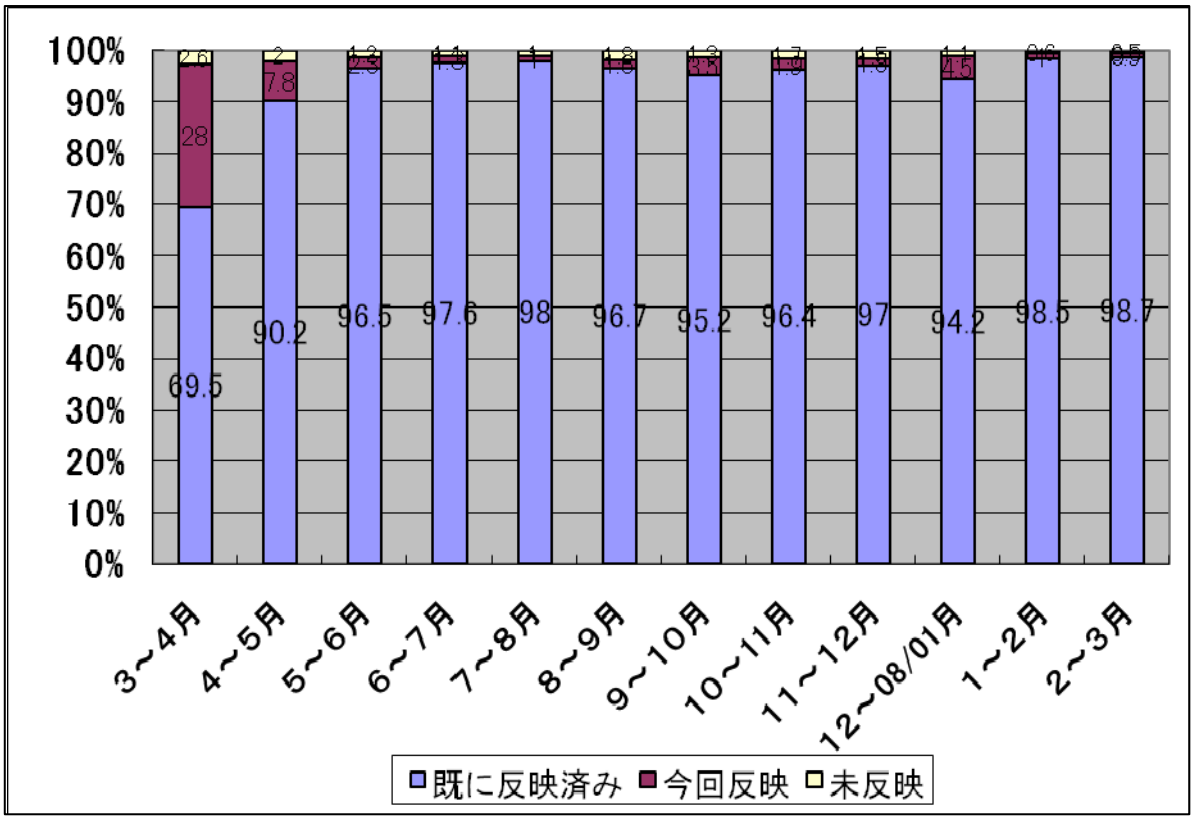
In November 2007, AhnLab Incorporated and Kaspersky Labs Japan Limited took part in the project as new members.

List of the Project Participating Security Vendors (alphabetical order)

- AhnLab Incorporated
- Kaspersky Labs Japan Limited
- McAfee Incorporated
- Microsoft Corporation
- Sourcenext Corporation
- Symantec Corporation
- Trend Micro Incorporated

4.3 Activity Achievements

Figure 4-1 shows the average figures between March 2007 and the end of March 2008 (reported between May 2007 and April 2008), indicating whether the Project Participating Security Vendors had already added detection for the samples collected by this project in the pattern files of their antivirus software (purple), added detection



this time (maroon), or had not yet added detection (yellow).

Figure 4-1: Change of Status of the Project Participating Security Vendors' Approaches

① It indicates slightly higher values for "Added detection this time" after October 2007 because CCC then shortened the schedule for passing samples.

② CCC converted the honeypots to support Windows XP in November 2007, which did not affect detection rates.

③ As one of the vendors had difficulties collecting data between December 2007 and January 2008, the values for "Added detection this time" were increased.

From these figures, the group infers that the collected samples have been fully utilized as one of the achievements of this project. Note that the group could determine that the samples registered in FY 2007 sufficiently contributed to preventing general users from becoming infected with BOTs, considering the combined total of the current Project Participating Security Vendors' shares amounted to 90% or more in Japan.

4.4 Future Activities

The group intends to continue to deal with this project in cooperation with the Project Participating Security Vendors to strictly manage the collected samples and promote the further detection of the samples in the pattern files of the antivirus software that the vendors are selling.

5 Summary

CCC believes that, in FY 2007, the three groups in the project committed themselves to BOT countermeasures in cooperation based on the activity results in the previous year.

The number of Project Participating ISPs increased from 8 ISPs in the beginning to 68 ISPs at the end of FY 2007. The disinfection tools have been modified to be effectively used by more users, by enhancing them—such as to support Windows Vista and adding additional functions. The Project Participating Security Vendors' share within Japan amounted to approximately 90% after the two newcomers joined the project in FY 2007. In addition, the media is being given more opportunity for coverage of CCC's work and the visibility of CCC is gradually being heightened.

Some indications suggesting how effective the countermeasures are have started to become clear, such as the decreasing number of users alerted by some of the Project Participating ISPs due to the group's work. At the same time, the functions of BOTs and infection methods are ever changing, and CCC must make continuing efforts to address such changes.

The activities of this project will continue in the future, aiming to make a significant contribution to realizing a safer and more secure Internet society.

6 Conclusion

~ To Minimize the Damage Caused by BOTs ~

Cyber Clean Center (CCC) recommends BOT countermeasures to minimize damage caused by BOTs.

Although there are no measures that can guarantee to completely prevent damage caused by infection of BOTs, you can minimize the risk by adopting the following countermeasures:

Infection Countermeasures

1. Keep your computer up to date
2. Ensure that you install antivirus software
3. Use a personal firewall
4. Use a broadband router for connection to the Internet
5. Do not preview mails in HTML format
6. Pay careful attention to e-mails with attached files (attachments)
7. Use authentication with IDs and strong passwords

CCC presents detailed instructions to the public at the following site:

https://www.ccc.go.jp/knowledge/index.html

Please, take appropriate virus countermeasures to protect the safety of your PC!