Countermeasures against Bots
Are you sure your computer is not infected with Bot?

IPA
Information-technology Promotion Agency
IT Security Center
http://www.ipa.go.jp/security/
1. What is a Bot?

Bot is a computer virus designed to control computers (infected with this virus) from an external source via a network (or the Internet). It waits for instructions from the external source and upon receiving them, performs programmed tasks. The name “Bot” was derived from “Robot”, as its functions are similar to those of robots.

2. Threats of Bot Network

Hundreds, thousands, or even millions of Bots can be placed under the control of a command-and-control server; this sort of network is called “Bot Network.”

If the Bot network is used for malicious purposes such as phishing (*1) fraud, transmission of a large volume of SPAM mails (*2), DDoS attacks (*3) to a specific site etc, it will become a big threat to us.
3. How Do They Infect Computer Systems?

The following are examples of how your system can be infected with a Bot.

1) Infected by opening a file attached to a virus mail

2) Infected by accessing a malicious Web site (containing a virus)

3) Infected by clicking a link (URL) contained in a Spam mail, which takes users to a malicious Web site

4) Infected due to a vulnerability (*4) in the computer allowing the virus to gain unauthorized access via the network.
5) Enters the computer system exploiting a Backdoor (*5) set by another virus

The following are other possible causes for your computer to be infected with viruses, so you need to be careful.

6) Infected by using file-swapping software (Pear to pear).

7) Infected by using the Instant Messenger (*6) service.

Case 4) is the case where users’ computers can be infected with viruses just by accessing the Internet. From the victims’ point of view, they do not even notice the infection as it happens without performing any operations. In such cases, not only you need to apply security patches using the Windows Update, but also take some measures to prevent unauthorized access via a network.

4. What Bots Do After Entering Your Computer System?

After entering your computer system, Bot will communicate with an external command-and-control server (in many cases, Internet Relay Chat (*7) is used by the Bots,) and upon receiving instructions, perform the programmed tasks (such as transmission of SPAM mails, DoS attacks (*3), network infection, Network Scanning (*8), etc.) In addition, they upgrade themselves and depending on the situation, change the command-and-control server from which they receive instructions.

Note, however, that these tasks are performed in the background without users’ knowledge, so it’s very difficult to cope with it.
1) Sending SPAM Mails (Sending a large volume of SPAM mails)

2) DoS Attack (Carrying out the Denial of Service Attack against a specified site)

3) Network Infection (Gaining unauthorized access to computers exploiting their vulnerabilities)
4) Network Scanning (Gathering information stored on computers by exploiting their vulnerabilities)

5) Self-upgrading and switching the command-and-control server from one server to another

6)Spying Activities (Transmitting information stored on a virus-infected computer to an external source)
5. How to Check for Bot Infection and Clean It?

(For Windows users)

Recent Bots use various techniques to carry out their tasks without letting users notice the infection. For example, when users attempt to update virus definition files for antivirus software, Bots can block it or even cause the program to abort. Bots use process names similar to the names of system-specific processes so users can hardly recognize them by viewing the process window, or even worse, the window does not open.

If you have any doubts, check for Bot infection using the following methods:

1) Keep the Computer Updated

Apply the Windows Update or Microsoft Update.

If you cannot access Microsoft Web sites, there is a possibility that access to the sites is being blocked by Bots or other viruses, so follow Instruction 3) below. If you find any wrong settings, correct them and apply the Windows or Microsoft Update again.

- Windows Update  
  http://windowsupdate.microsoft.com/
- Office Update  
  http://office.microsoft.com/ja-jp/officeupdate/
- Microsoft Update  
  http://update.microsoft.com/microsoftupdate/

For information on how to apply the Windows Update or Office Update, please refer to the following Web sites:

- How to apply the Windows Update  
- How to apply the Office Update  
- How to apply the Microsoft Update  
If you run the Windows Update or Microsoft Update, the Malicious Software Removal Tool is also activated. This tool scans your computer for various Bot programs and removes them if detected. In a sense, it’s like using free software to clear malicious programs. However, this is only done when the Windows Update or Microsoft Update is performed; so if necessary, download the tool from the Microsoft Download site. Once this is done, you can use it any time you want.

- Malicious Software Removal Tool
  http://www.microsoft.com/japan/security/malwareremove/default.mspx

2) Scan for Viruses Using the Latest Virus Definition Files

If you are using antivirus software, keep its virus definition files up-to-date so you can properly scan your computer for viruses.

If you are not using any antivirus software, use free-online scan services provided by some vendors. (Refer to page 12)

If you cannot access the vendors’ Web sites, there is a possibility that access to the sites is being blocked by Bots or other viruses, so follow step 3) below. If you find any wrong settings, correct them and recheck for viruses, using the software or free-online scan service with its virus definition files updated.

Note: Some viruses might not be removed by online-scan services. In such cases, you need to do it manually by following the instructions provided for each virus.

Antivirus software is shifting towards the Integrated Security Management Software, which provides firewall functionality to protect against virus infection over a network.

Even in the case where your PC has already been infected with a Bot, outgoing access carried out without your knowledge can be monitored and blocked, so you can notice that your PC has been infected with the malicious program. It is an important measure to use such security software.
3) Check the following file:

- HOSTS file
  For Windows NT and 2000 users:
    The HOSTS file located in the folder C:\WINNT\SYSTEM32\DRIVERS\ETC
  For Windows XP users:
    The HOSTS file located in the folder C:\WINDOWS\SYSTEM32\DRIVERS\ETC

- To check the contents of the file, you can use the Notepad program (notepad.exe).
  The HOSTS file is used to identify the IP address of the computer you are going to connect.

Attacker can alter the mappings so that your computer is connected to a wrong IP address, when it tries to access the URL of a specific Web site.

If the file has not been edited, it must contain only the “localhost” as shown below. If this is not the case, check for the following points:

- If the file contains the URLs of Microsoft Web sites or the Web sites of antivirus software vendors, you need to delete them. (“127.0.0.1 localhost” indicates that it’s the computer your are using)
The following is an example of mappings tampered by an attacker.

127.0.0.1  www.microsoft.com
127.0.0.1  www.nai.com
127.0.0.1  trendmicro.com
127.0.0.1  update.symantec.com
127.0.0.1  updates.symantec.com

If the line begins with “#”, it is a comment, so you don’t have to worry about it.

6. Points to be Noted by General Users

General users using a network (the Internet) should take the following measures to protect against Bot or virus infection.

(1) Installation of Security Software
Install security software (such as antivirus, anti-Spyware, Integrated Security Management software etc) and update its virus definition files on a regular basis, and then perform a virus scan on your computer.

(2) Be careful about files attached to emails
Do not easily open files attached to emails from unknown sources. Especially, be careful about executable attachments.

(3) Refrain from visiting suspicious Web sites
There are some Web sites designed to embed malicious programs onto users’ computers. It is too risky to visit these sites having no security mechanism.
(4) Effective use of the Internet Options (Security Options) supplied with a browser

Classify Web sites into secure and insecure groups, and set the security level higher if you are going to visit insecure sites.

- Ensure the Security with Internet Explorer (Microsoft)

(5) Do not click any tempting links contained in SPAM mails

Be careful about tempting links contained in SPAM mails. Clicking such links will take you to a suspicious Web site as explained in (3) above.
(6) For secure Internet access, install a router or personal firewall, configure and operate it in an appropriate manner.

For secure Internet access, it is recommended to use a router or personal firewall to protect your computer and network from virus-infection. In doing so, even if your PC has already been infected with a virus, you can prevent the leakage of data over the Internet that is stored on your computer or transmitted on a Network.

(7) Keep your operating system and applications updated (by performing Windows Update)

7. Points for Web Operators to Protect against Bots

Web operators and other users using the Internet to provide information should take the following countermeasures, so they can prevent their computers from being abused by Bots or other computer viruses as a stepping stone.

(1) Protect your Web pages from being hacked, defaced, or infected with viruses, which can install Bots.
(2) Keep your operating system and applications updated.
(3) If you find something unusual, close down your Web site and do whatever you can to prevent the damage from spreading.
8. References

For further information, please refer to the following materials:

- **IT Security White Paper 2006 (Japanese Only)**
  http://www.ipa.go.jp/security/vuln/20060322_ISwhitepaper.html
- **Computer Security 2004 Trends and Countermeasures**
- **Information on Antivirus Software**
  http://www.ipa.go.jp/security/antivirus/vacc-info.html
- **Malicious Software Removal Tool**
  http://www.microsoft.com/japan/security/malwareremove/default.mspx
- **Be Careful About Botnet**

**Online Scan (Virus Scanning Service)**

- Symantec Security Check
  http://www.symantec.com/region/jp/securitycheck/
- Trendmicro Online Scan
  http://www.trendmicro.co.jp/hcall/
- McAfee Free Scan

**IPA Countermeasure Guides Series**
http://www.ipa.go.jp/security/antivirus/shiori.html

- IPA Countermeasure Guide (1) Countermeasures against Virus
- IPA Countermeasure Guide (2) Countermeasures against Spyware
- **IPA Countermeasure Guide (3) Countermeasures against Bots**
- IPA Countermeasure Guide (4) Countermeasures against Unauthorized Access
- IPA Countermeasure Guide (5) Countermeasures against Information Leakage
9. Terminology

(*1) Phishing
A type of fraud whereby a criminal sends fake emails claiming to be a legitimate financial institute (such as bank, credit-card company etc), in an attempt to acquire recipients’ personal information (such as names, addresses, bank account numbers, credit card numbers etc.) The name “phishing” was derived from “fishing”, as its sophisticated technique is similar to the one used for fishing.

(*2) SPAM mail
Also called Unsolicited Bulk Email (UBE). Emails containing identical or nearly identical messages that are sent to any number of recipients for commercial, religious, or harassing purposes.

(*3) DoS / DDoS Attack
Denial of Service Attack that causes a loss of services to users, by overloading the computer system connected to a network, exploiting the characteristics of the Internet protocol. If multiple devices are used as a source of denial-of-service attacks against a single computer, the load will become much heavier. This attack is called the Distributed Denial-of-Service (DDoS) Attack.

The source of a DDoS attack can be a Web site exploited by an attacker; it means that he might embed malicious code into some Web sites so he can remotely run the code to carryout simultaneous DDoS attacks.

(*4) Vulnerability
Vulnerability in terms of information security is a security hole that may degrade the security level of systems, networks, applications and protocols, which can bring unexpected, unwanted events, or design and implementation errors. Vulnerabilities are classified into “vulnerabilities in the operating systems”, “vulnerabilities in applications”, etc. Inadequate security settings are also referred to as vulnerability. In general terms, it is called “security hole”.

(*5) Backdoor
A program that is installed by an attacker to enable him to come back into the computer at a later time without having to supply login credentials or going through any type of authorization. Attackers use a port available on the computer.
(*6) **Instant Messenger (IM)**
A Software program that enables chat and file-swapping between computers connected to the Internet. Before sending real-time messages, you can check whether the other computer is connected to the Internet. Among popular ones are AOL Instant Messaging and MSN Messenger.

(*7) **Internet Relay Chat (IRC)**
Chat system. By accessing an IRC server on the Internet using dedicated software, you can exchange messages with multiple users.

(*8) **Network Scanning**
Activity of checking services available from ports on a computer, in which a method called “Port Scan” is used. It can detect whether a backdoor, installed by another virus, is running.

---

We enlisted cooperation from the following organizations in creating and publishing this guide.

- **Symantec**

- **Trendmicro**
  [http://www.trendmicro.co.jp/](http://www.trendmicro.co.jp/)

- **McAfee Japan**