SCIS2000 The 2000 Symposium on Cryptography and Information Security
Okinawa, Japan, January 26-28, 2000

SCIS2000-D.III.8

Trends of Malicious Codes and their Countermeasures

Kyu-beom Hwang* Kwangjo Kim* Joonsang Beak*, Charles Ahn**
kwangkb@ahnlab.co.kr kkj@icu.ac.kr mohi@icu.ac.kr csahn@ahnlab.co.kr

Abstract- Due to current damages caused by various malicious codes, the protection of computer or storage systems from malicious codes are considered to be of utmost importance, in addition to the protection of information itself. Recently, there has been a great increase in a number of damages cases by malicious codes and the distribution of worms through e-mails has frequently occurred. In this paper, we study concepts of various malicious codes including viruses, Trojan Horses, and worms. We also propose a new classification of such malicious codes and analyze trends of the malicious codes discovered in Korea and Japan. Also, we discuss how to countermeasure from malicious codes.

Keywords: Computer Anti-Virus, Malicious codes, Malware, Malcodes

I. Introduction

In April 26th 1999, CIH virus has largely damaged computer systems in most Asian countries. The damage might be from most computer users' indifference rather than deficiency of anti-virus technologies or countermeasure against the computer viruses[7].

According to the reports published in Korea and Japan each year, the damages by malicious codes including computer viruses have become serious to cause trouble in business and information systems exceeding the level of practical jokes of virus makers.

In this paper, we define internet worms, Trojan Horses and analyze such malicious codes including discovered viruses and survey their trends. Also, we propose countermeasures against them.

This paper is organized as follows. Definitions of computer viruses and their structural elements are given in Section 2. Major patterns of the damages made by computer viruses are analyzed in Section 3 and routes of propagation are described in Section 4. In Section 5, we discuss prevention of the malicious codes including the computer viruses and concluding remarks will follow in the final Section.

II. Definitions of malicious codes

1. Definition of malicious codes

Malicious codes(in short, 'malcodes') are defined as all kinds of executable programs, macros, or scripts that are produced in order to intentionally damage computer systems. Thus, bugs occurred by programmers mistakes, which are not intentionally produced are excluded in the category of malcodes. However the bugs being really harmful to computer users are sometimes categorized as malcodes[6].

The name of malcodes are given by virus naming rules. We will classify malcodes into viruses, worms, and Trojan Horses and uses their name in underlined italics font to distinguish with other normal text, *e.g.*, *Melissa*.

In the past, the term "Malware(Malicious Software)" was used instead of "malcodes". However, the meaning of Malware was too narrow to include the hoax e-mail which is not exactly software but should be included in the category. Hence we use the term "codes" instead of software.

In this paper, we deal with the issues related to malcodes which exist in MS-DOS and MS-Windows.

2. Classification of malcodes

The malcodes can be classified into viruses, worms, and Trojan Horses and includes some programs which contains bugs.

2.1 Viruses

Viruses are said to have a malicious capability to reproduce themselves and contain sets of codes that modify executing or internal structure of target codes to run viruses before executing. Viruses may have harmful side effects such as display of some curious messages, deletion of C-MOS memory data, and destruction of information in hard disks and etc. The side effects are becoming more and more serious[2]. The examples of the computer viruses are *Brain*, *One_half*, *Die_Hard*, *XM/Laroux*, and famous *Win95/CIH*.

2.2 Worms

In 1970s, worms were referred to programs that copy themselves into only memory storages of large

* School of Engineering, Information and Communications Univ., 58-4 Hwaam-dong, Yusong-gu, Taejon, 305-348, Korea
** Dr. Ahn's Anti-Virus Laboratories, Inc., 10F Samhwa Bldg., 144-17 Samsung-dong, Kangnam-gu, Seoul, 135-745, Korea

sized computers. Recently, they however are referred to propagated executable codes that are running in small sized computers such as PCs. We restrict ourselves to deal with such worms occurred in PCs. The main distinction between virus and worm is whether they have infected target codes, *i.e.*, even though virus possesses the target codes, worm does not have the target codes[1].

The typical worms discovered in Korea and Japan are *I-Worm/Happy99(Ska)*, *I-Worm/ExploreZIP*, *I-Worm/PrettyPark*, and *I-Worm/MyPics*.

2.3 Trojan Horses

Trojan Horses are produced with malicious intention. Different from viruses, they do not a capability of self-reproducing. Trojan Horses may be distributed with other utility programs including them or distributed as an utility program itself. Trojan Horses can outflow or destruct user's information.

The examples of Trojan Horses are *Win-Trojan/Back_Orifice*, *Win-Trojan/SubSeven* and *Win-Trojan/Ecokys(Korean).*

3. Sub-Classification of malcodes

Except for viruses, malcodes are not further sub-classified due to small number of cases. However we further classify worms and Trojan Horses. In this paper, we propose some methods for sub-classification.

3.1 Classification of Viruses

In general, viruses are classified according to infected regions where virus codes are located. Following the regions, viruses are divided into 4 categories, boot virus, file virus, multipartite virus, and macro virus[3].

- Boot virus

If a computer is powered on, an initial program in boot sectors is executed. The virus located in boot sectors is called boot virus.

- File Virus

File virus refers to a virus that infects executable programs It is noted that about 80% of all viruses are file viruses.

- Multipartite Virus

Multipartite virus infects both a boot sector and files. The damage caused by multipartite virus is very severe.

- Macro Virus

Macro virus is recently discovered. It's targets are not executable files but document files used in Microsoft Excel or Word programs. It starts to infect when the application program reads document files containing macros.

3.2. Classification of Trojan Horses

Trojan Horses are classified as execution environments such as operating systems in which they are running. They have been classified as DOS Trojan Horse and Windows Trojan Horse.

- DOS Trojan Horse

DOS Trojan Horse is running in DOS. It declines the speed of computers or deletes files in specific days or situations.

- Windows Trojan Horse

Windows Trojan Horse is executed in Microsoft Windows systems. The number of Windows Trojan Horse has increased since 1998 and has been operated as malicious hacking programs that collects information in computer systems connected by network such as Internet.

3.3. Classification of Worms

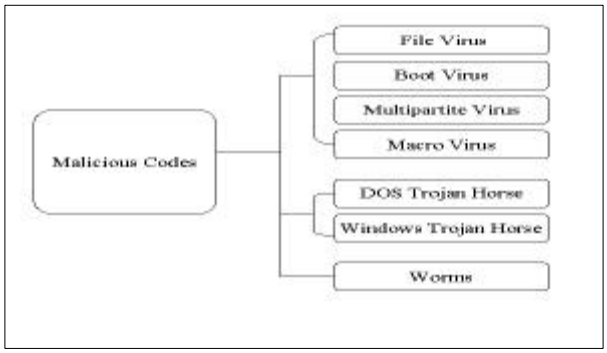
Worms were considered to be not important in PCs but have widely been known to public since the worms transmitted by e-mails appeared in 1999. Because there are small number of worms appeared, there is no specific classification method for worms.

3.4. Proposed classification method for malcodes

Malcodes are classified as Fig. 1 by mixing methods for classification of 4 major elements, viruses, worms, and Trojan Horses. This new classification method can make use of existing classification and it is not difficult to re-classify Trojan Horses and worms when other way of new classification is proposed.

III. Major Trends

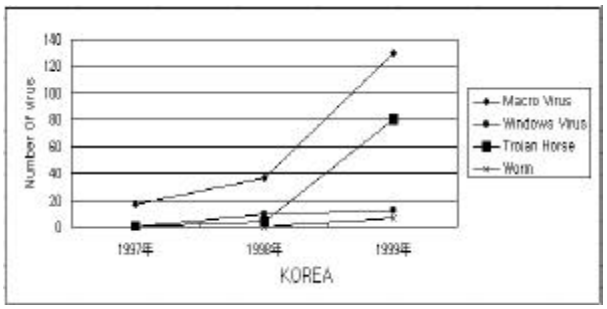
The recent malcodes which are frequently discovered are macro viruses, script viruses, and worms delivered by e-mails. The virus executing in JAVA environments are also discovered[5].



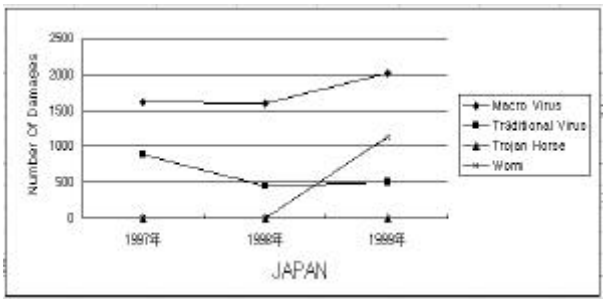
<Figure 1> Proposed classification of malcodes

The methods of computing statistics the frequency of virus emergence in Korea and Japan are different. The statistics are based on the number of individual viruses and on the number of damages in Korea[8](Fig. 2) and Japan[9](Fig.3),

respectively.



<Figure 2> Increase of Viruses in Korea

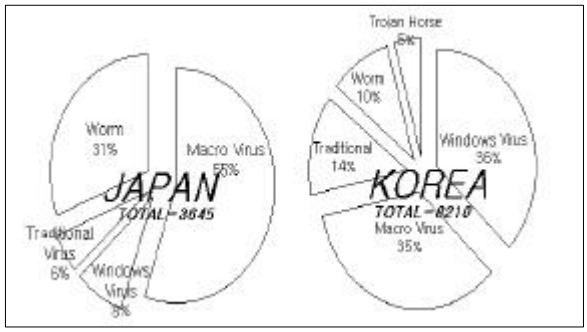


<Figure 3> Increase of Damages by Malcodes in Japan

Note that there was an upsurge of increase in the number of malcodes in 1999 compared to 1998, in both countries.

Since Trojan Horses are regarded as being included in viruses in the statistics of Japan, we discounted them for comparing to the statistics of Korea in which Trojan Horses are excluded. To approximately measure the number of damages by viruses in Korea, we used the data that represents the number of cases of virus damage-counseling.

Fig. 4 shows a pattern analysis of malcodes' damage reporting in Japan and Korea. As can be seen, larger percentages of damages are made by macro viruses(55%) and worms(31%) in Japan. On the other hand, Windows viruses(36%) are the biggest damage in Korea and the percentage of damages by macro viruses(35%) are smaller than that of Japan. Also, the damage by worms is relatively small(10%) in Korea.

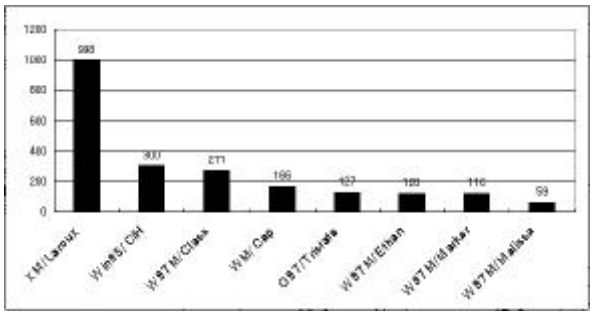


<Figure 4> Ratio of virus damages in Japan and Korea

1. Trend of Virus

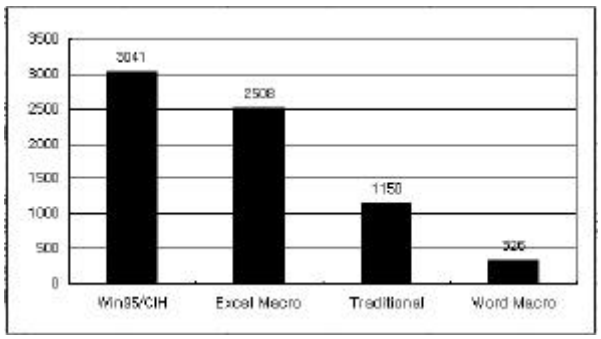
Recently, a number of macro viruses have explosively increased and a scale of damages have enlarged. It comes from the reason why there are many people using Microsoft Excel or Word and the propagation of the viruses has become extremely fast due to easy information propagating means tools such as Internet.

Though *XM/Laroux* was the most frequent virus in Japan(46.8% in 1998), the number was reduced(27% in 1999). Consequently, *Win95/CIH*, *W97M/Class* and *WM/CAP* were three major damages in 1999 and as a whole, the damages by macro virus looks outstanding. (Fig. 5)



<Figure 5> Major virus damage reporting in Japan, 1999

In Korea, the largest number of damages was made by *Win95/CIH*. The number of virus damage-counseling cases was 3041 and this was the 36% of all number of damage-counseling. The second largest was Excel Macro Virus(30%), the third was Traditional Virus(14%) , and Word Macro Virus(5%). (Fig. 6)



<Figure 6> Major virus counsel report in Korea

To sum up, the damages by macro viruses are most severe in Japan but Windows viruses are major concern in Korea.

X97M/Extras macro virus that has polymorphic method and *W97M/Class* macro virus that has both polymorphic and stealth methods are also discovered. The macro viruses such *W97M/Melissa* that transmits infected documents to damage recipients through MS-OutLook e-mail client system are also discovered. It is predicted that

modified macro viruses activating in MS Office 2000 will appear in the near future. It is also predicted that the viruses that use higher techniques such as polymorphic and stealth method will appear.

Windows viruses such as *Win95/CIH* making systems dumb have recently discovered. The damages caused by these viruses are very serious.

The number of individual viruses has constantly increased since 1992 and as a result there are hundreds of Windows virus in nowadays. It is considered that the advent of Windows 95 has accelerated the rate of Windows viruses infection. Windows virus start from *Win16/Tentacle*, *Win16/Tentacle.II*, *Win95/Anxiety_Poppy* which are Windows 95 memory resident virus, and evolve into *Win95/HPS(or Hanta)* which has polymorphic method, respectively. In late 1999, *Win32/Kriz* that makes systems dumb like *CIH* was found but no instance of damages was reported.

Recently, *Win95/Love* that sends out famous commercial signal music was discovered during the provision for Y2K but there were no additional damages. In Japan, it was reported that no viruses were found in that period.

The damages caused by *Win95/CIH* have relatively been decreased. However, viruses not only make use of compression methods but also modify themselves to other forms will be very likely to appear. Also, the open of *Win95/CIH* virus-source code to public will help in appearing other modified versions of *Win95/CIH* virus.

2. Trend of Trojan Horses

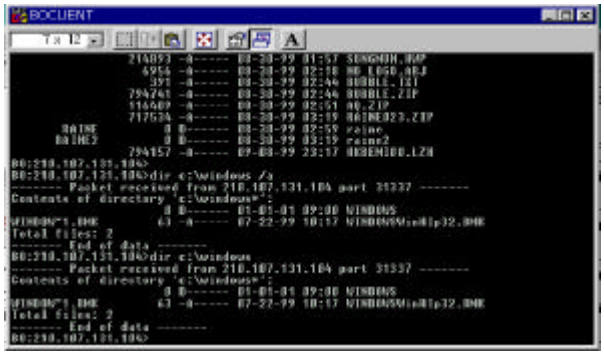
Trojan Horses are mostly used to extract information from computer systems. In July, 1999, *Win-Trojan/Back_Orifice_2000* executing in Windows NT and Windows 95 systems was distributed. Then many people are concerned about inadvertent outflow of their information. Since the source code of *Back_Orifice_2000* was open to public, it is very probable that it can be further developed to stronger version and in fact, 40 different modifications have discovered within 5 months.

Also, it was reported an accident that a criminal extract information about home-banking account and password using Trojan Horse from other's computers.

Fig. 7 shows the execution of the *Back_Orifice_2000*. Using it, one can easily access others' computers remotely and bring information into his system. It is also reported that the distribution of *Back_Orifice_2000* or its modified versions is being done by hacking sites.

If a plug-in program, "Butt Trumpet 2000" is included in *Back_Orifice_2000*, it tells the fact that *Back_Orifice_2000* is being executed to the assigned e-mail address. Therefore, it is not necessary for the attacker to make sure which system contains *Back_Orifice*.

Since *Back_Orifice* can encrypt transmitted data, modify/extract users' information, care should be taken. Most of *Back_Orifices* are now prevented by anti-virus vaccines but it is predicted that compressed or extremely modified versions of them will occur in the near future.



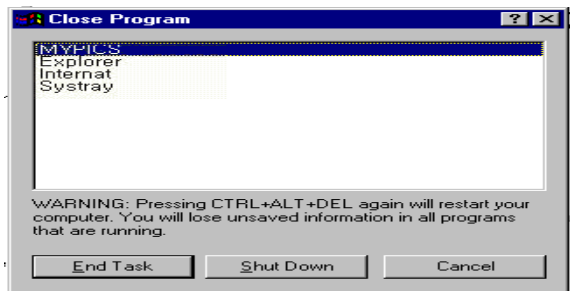
<Figure 7> The execution of Back Orifice Client

3. Trend of internet worm

In Asian countries, there were a lot of damages by worms through Internet in 1999. The Internet worms include *I-Worm/Ska(Happy99)* that are attached to e-mails, which can modify socket library in Windows systems and *I-Worm/ExploreZIP* that are transmitted by users replying received mail and seriously damages MS Office documents files and program sources. Also, *I-Worm/PrettyPark* that outflows individuals' e-mail addresses and passwords is discovered in September, 1999.

I-Worm/MyPics, recently discovered Internet worm, orders AUTOEXEC.BAT to execute FORMAT.COM. Thus all the information in harddisks will be format at the time of next booting of the computer. *I-Worm/MyPics* propagates through e-mails, as a result, damages seriously.

Fig. 8 depicts the execution of *I-Worm/MyPics* using Windows 95's close-program window(similar Japanese Windows 95)

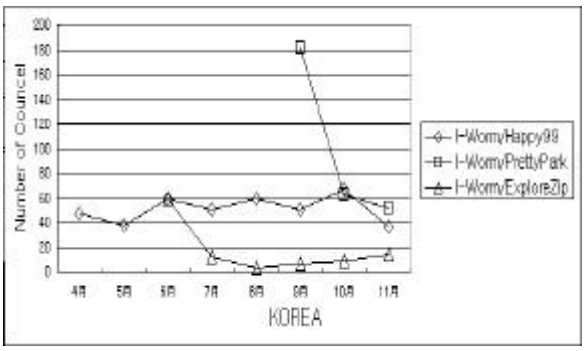


<Figure 8> The execution of *MyPics*

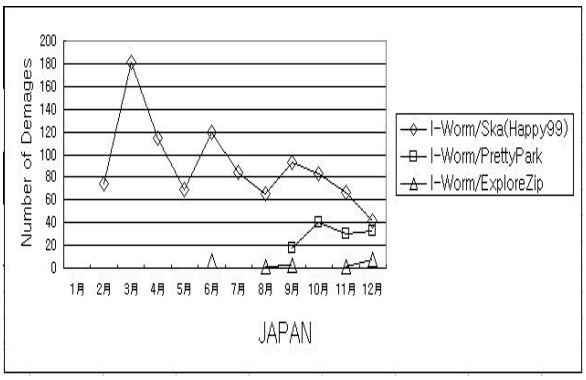
The worms through e-mails are transmitted by two forms. One is an attached file to a transmitted

message, which has stealthily been added to the message. The other disguises as an useful utility. The problem of the worms through e-mails is that it is too fast to prevent their propagation.

The damages by worms have increased in both Korea(Fig. 9) and Japan(Fig. 10).



<Figure 9> Number of Worm's Damages in Korea



<Figure 10> Number of Worm's Damages in Japan

Though *I-Worm/ExploreZip*, *I-Worm/ExploreZip.Pak* and *I-Worm/MyPics* are not frequently founded, it was reported that the damage by such worms was very severe. The new types of worms will be transmitted through e-mails[10][11].

IV. The route of propagation

The routes of inflow of malcodes in Korea and Japan are very different. In Korea where most networking is made through access to ISP(Internet Service Provider)s by telephoning, malcodes are mostly propagated through 'PC Communication Network'. On the other hand, in Japan, malcodes are mostly propagated through e-mails, storage media from outside, enterprise network environments such as intranet[4].

In this Section, we further investigate the route of inflow of malcodes, dividing 3 categories. The first route is an inflow of malcodes masqueraded as utility programs. The second route is an exchange or a share of data containing malcodes. The last route is through e-mails.

1. Malcodes masqueraded as utility programs

In Korea, for example, viruses are distributed as latest versions of utility programs masqueraded as famous vaccine programs such as V3+ and M-DIR or as shareware programs crack program as registered ones. These malcodes are widely spreaded and made many systems damaged at once.

Since *CIH*, which recently attacked Asian countries, was also distributed as an utility program, a wide infection was possible.

Another example is a distribution of *Back Orifice 2000* which are known to users as a new Windows utility.

The hacking tool such as *Back Orifice 2000* is often included in the programs that are registered in the World Wide Web sites or the pirated software products.

2. Propagation of malcodes through information exchanges

The flow of viruses through information exchange is not execution of programs but exchange of data files such as word processor or spreadsheet document files. It should be noted that users who use right software can be exposed to viruses.

Document files are exchanged in companies or government offices on the belief that all entities are honest. Hence the targets of macro viruses are not individual users but group users. Also, macro viruses are usually from foreign countries and hence university or global companies are more vulnerable to be attacked. And it is predicted that new modification followed by new Microsoft Office will advent.

3. Worms and Trojan Horses through e-mails

Recently, worms and Trojan Horses are propagated through e-mails. In particular, attackers masquerade themselves as trusted senders and recipients execute attached malcodes without doubt and, as a result, they are seriously damaged. In 1999, various kids of worms are distributed through e-mails. These internet worms can be attached to e-mails by modifying Windows socket library or registration information in registry.

The most latest internet worms are destructive like *I-Worm/ExploreZip* and *I-Worm/MyPics* and harmful to psychological anxiety like *I-Worm/Ska(Happy99)*.

V. Countermeasures

The best way to reduce the damages of malcodes

is to make attention and do prevention. The best prevention at present is cutting off document files or programs from outside. Most viruses are not imported by internal users but by the malicious external users. Therefore, if such inflow is originally cut off, one can be safe from viruses. But complete isolation of the information channel is impossible and is ineffective since information exchange is fundamental in today's computing environments. Hence an effective use of vaccine programs or information from mass media may be more practical.

Though many vaccine researchers have been studying new technologies for protection from computer viruses for many years, there has not yet occurred revolutional method. Hence it is undesirable to depend on vaccine programs. If one wants to use shareware software products, one should directly visit the web sites of the companies that produce the shareware programs and download such programs. Also, one should not execute programs and executable files attached to e-mail messages if they are not fully confirmed. Of course, one should keep in mind that such programs may be very harmful to computer systems or other programs.

It should also be noted that some agencies are providing information about malcodes including computer viruses. The information providing agencies include, for example, KISA (Korea Information Security Agency,http:\\www.kisa.or.kr), AHNLAB (Dr. Ahn's Anti-Virus Laboratories, Inc., http:\\www.ahnlab.com) in Korea, IPA(Information-Technology Promotion Agency, http:\\www.ipa.go.jp), JCSA(Japan Computer Security Asscocitation, http:\\www.jcsa.or.jp) and vaccine producing companies in Japan.

It is world-widely recommended that the latest versions of vaccine programs should be used and data from outside should be investigated completely. It is also recommended that the programs attached to e-mail messages should not be executed. In network environments, the access permissions of all programs should be set up as read-only except those of system administrator's and unnecessary shares of data should be avoided. If one keeps above recommendations, more 80% of safety of data or programs is guaranteed.

Furthermore, the additional use of cryptographic technologies such as an authentication of data or a digital signature to confirm exchanged data guarantees more safety.

Ⅵ. Conclusion

After reviewing concepts of various malcodes including viruses, Trojan Horses, and worms, we have proposed a classification of such malcodes and analyzed trends of the malcodes in Korea and Japan. Also, we have discussed protection of computer systems from malcodes.

Due to the development of malcodes techniques, the damages caused by malcodes are more and more severe. Almost all malcodes techniques(negatively), which were claimed as methods for system weakness by the makers, are now far from good intension. The good examples are *Win95/CIH*, *W97M/Malissa* and *Win-Trojan/Back_Orifice*. However, mass media sometimes report the malcodes technique(negatively) as a great technology and, as a result, some encouraged computer mania who want to be heros make such malcodes. Thus such way of reporting should be avoided.

Security of information itself is important. But protection of computer systems that produces and stores information from malcodes such as viruses, Trojan Horses, worms is more important.

We suggest information protection against malcodes using cryptographic technologies as our future research.

References

[1] R. Burger, Computer Viruses a high-tech disease, Abacus, 1988.

[2] Ralf Burger, Computer Viruses and Data Protection, Abacus, 1991.

[3] Chalres Ahn, Virus Analysis and Vaccine Programming, Information Age Co., Ltd., 1994.

[4] Charles Ahn, Virus Prevention and Repairing, Information Age Co., Ltd., 1997.

[5] Kyu-beom Hwang, Kwangjo Kim, Charles Ahn, "Analysis Computer Virus Schemes and Current Status", Proceeding of KIISC(Korea Institute of Information Security and Cryptology) Conf. Chung-Cheong, Korea, , Oct. 1999.

[6] Kyu-beom Hwang, Kwangjo Kim, Charles Ahn, "Analysis Malicious Code Schemes and Current Status", Proceeding of CISC 99, Korea, pp.202-215, Nov. 1999.

[7] Kyu-beom Hwang, Kwangjo Kim, Charles Ahn, "Analysis and Recovery of CIH virus", To appear KIISC Journal.

[8] AHNLAB, http:/www.ahnlab.com

[9] IPA, http://www.ipa.go.jp/SECURITY/txt

[10] http://www.ipa.go.jp/SECURITY/topic

[11] http://www.virusbtn.com/WildLists/200001.html