2006

An Efficient Control of Virus Propagation

Madihah Mohd Saudi
National ICT Security & Emergency Response Centre (NISER), madihah@niser.org.my

Shaharudin Ismail
Islamic University College of Malaysia (KUIM), shaharudin@admin.kuim.edu.my

An Efficient Control of Virus Propagation

Madihah Mohd Saudi
National ICT Security & Emergency Response Centre (NISER)
Malaysia
madihah@niser.org.my
Shaharudin Ismail
Islamic University College of Malaysia (KUIM)
Malaysia
shaharudin@admin.kuim.edu.my

Abstract

There are very few studies done in dealing with computer viruses in Malaysia. By realizing that, this research paper is done in managing of virus problem among ICT users in Malaysia. Firstly, this research is establishing the existence of the problem through a questionnaire survey, which was carried out specifically at Klang Valley and Putrajaya in Malaysia. Then a study was made on classifying virus, studying their symptoms and behaviour with the aim of controlling its propagation by studying their known features. The ECOVP (Efficient Control of Virus Propagation) system that was developed is capable of educating users in handling computer virus incidents and at the same time helps to control computer virus propagation.

Keywords: Computer virus, worm, virus propagation, virus incidents

1. Introduction

Computer viruses have become real threats for computer users in the past few years. However, only few studies have been done trying to map out how large the problem actually is. In Malaysia, very few studies were done in dealing with computer viruses. The computer viruses problems in Malaysia caused big financial loss and it took an average of 1-2 months to eradicate virus and worm problems (Iman 2003; Saudi 2004). In the past, the distribution of anti-virus signature files required extensive periods of time to ensue (The Honeynet Project 2002) compared to the speed of spread of today's viruses and worms worldwide less than half of that time. This has raised the question of any other alternative ways in helping the society to reduce the loss of money especially when confronting with virus attacks? Currently, only few systems are capable of providing users step-by-step procedures in handling computer virus incidents. In order to handle a computer virus incident properly, the user awareness and education about computer viruses need an in-depth research (Kephart and White 2001; Perry 2002). A system that is capable to guide users on how to handle virus incidents following the incident response procedures need to be developed. These reasons give a sense of urgency for this study.

2. The Problems

Several important aspects of computer viruses problem should be acknowledged and need an in-depth study in order to understand the problems. Hundreds of different computer viruses are written every day, and their numbers are increasing rapidly. Based on the observation and research done by others, below are the identified problems:

- User has no knowledge about computer viruses and having difficulties confronting virus incidents.
- Lack of research related with user education of computer viruses in Malaysia.
- Need an efficient and an effective system that has standard operating procedure in handling computer viruses incident.

3. Questionnaire Survey

For the purpose of this study, the computer viruses awareness is defined and referred as having knowledge and understanding on how virus spread or also known as the channel of transmission for virus spread, the reaction and response that should be taken once infected with virus, the computer virus eradication procedure, the anti-virus functionality, capabilities and issues and the media channel of receiving the virus information. Meanwhile, the computer viruses impact is referred as the damage computer viruses have caused and how it affects user daily operation. The impact is similar to the payload of computer viruses. Viruses can do any kind of damage that software can do. This includes overwriting data, erasing files, scrambling system information, reformatting disks, disabling security systems or killing program processes. The other examples of the impacts caused by the computer virus are loss of data, loss of trust and reputation, information compromise, loss of customers, loss of loyalty and retention, loss of Web site, loss of time and loss of money. In term of financial loss, in Malaysia the financial estimated loss to due Code Red and Nimda outbreak was RM21 million and RM31 million estimated lost due to Blaster and Nachi (Saudi 2004).

The objective of the questionnaire survey is to study and analyze the computer viruses awareness among users, the prevention levels in organizations and the impact computer viruses have caused in Klang Valley and Putrajaya. The sampling was chosen based on total subscribers of the Internet, location of the place for example located in urban area and as the federal government administrative and business centre in Malaysia. The Eight Malaysia Plan (2001 - 2005) shows that 53.6 percent of the total Internet subscribers are concentrated in the Klang Valley. Kuala Lumpur registers the highest penetration rate with 103.9 subscribers per 1000 people, followed by Selangor with 84.9 per thousand respectively. R. Ramachandran, NITC Secretariat held the disparity measure showed that these developed states; Kuala Lumpur and Selangor are above national level. Putrajaya was chosen as the sampling population as it is the federal administrative centre of Malaysia. It is also located within the Multimedia Super Corridor (MSC) and it is set to be a model garden city with sophisticated information network based on multimedia technologies.

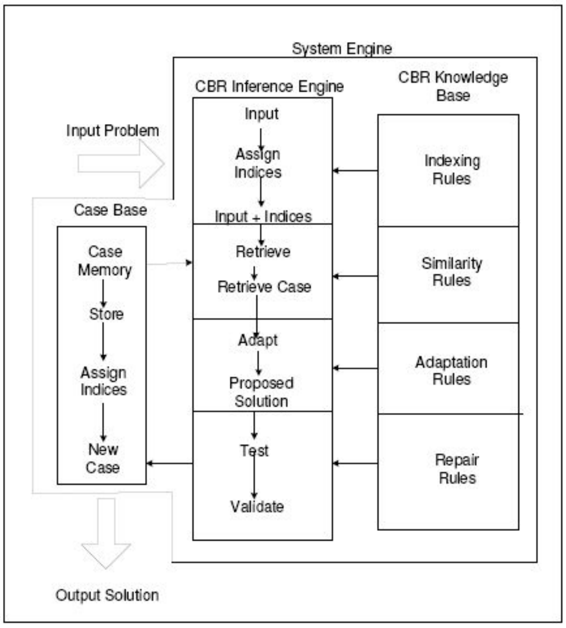
4. The Efficient Control of Virus Propagation (ECOVP) System

The ECOVP system is considered as capable to educate user about computer viruses and helps to control computer virus propagation. The interactive system that is easy to use, easy to learn, easy to understand, efficient and effective are the principles used for the system design. The system consists of problem solving and guidelines on how to handle virus incidents. The solution provided based on the symptoms given by the user later will be diagnosed by the system using the case based reasoning technique. The user will rectify his machine based on solution recommended by the system. User succeeds in rectifying and following the instruction given by the system, helps to control the virus propagation. The existence of the ECOVP system also helps to minimize the damage caused by the viruses and user ICT usage is supported by this ECOVP system**.**

5. The ECOVP System Design

Basically the ECOVP system consists of three (3) main features. The features are the Input Problem, System Engine and Output Solution. The system design diagram is displayed in figure 1 below.

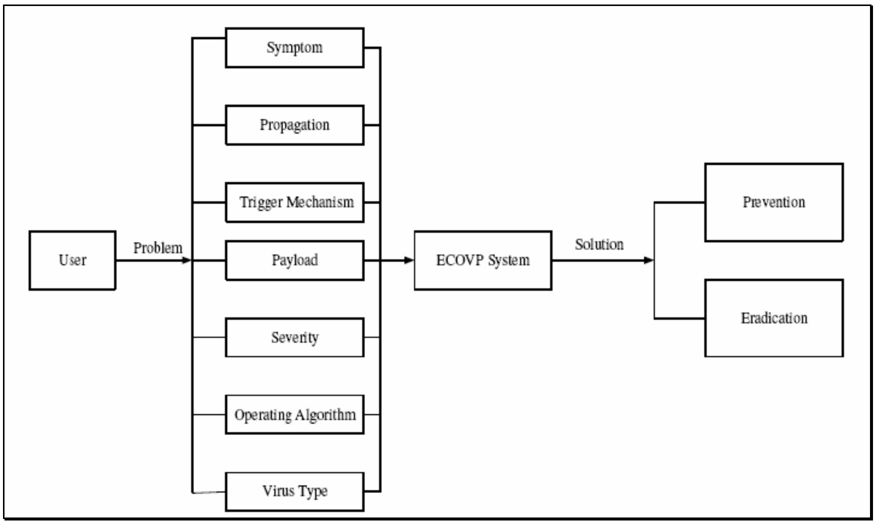
Figure 1
System Design for the ECOVP system



5.1 Input Problem

The Input Problem is the input from user that contributes to variety of prevention and eradication procedure solutions. Basically the input problem is based on the seven (7) ECOVP computer viruses classification namely symptom, propagation, mechanism trigger, payload, severity, operating algorithm, and virus type. The whole processes which starts with the input from the user and the solution as the output as illustrated is figure 2.

Figure 2
Input Problem and Output Solution



5.2 System Engine

The ECOVP's System Engine consists of three (3) components as the following:

a. ***Case Base***: It is the database of the cases.
b. ***Inference Engine***: Also known as the management of reasoning that consists of retrieves, reuse and revise processes.
c. ***Knowledge Base***: It is how the representation of the cases. Rules are assigned for each input. Generally the rules of the Knowledge Base component are Indexing Rules, Similarity Rules, Adaptation Rules, and Repair rule.

5.3 Output Solution

This component will display the solution (consists of the prevention procedure and eradication procedure) to the users. The solution is also part of the domain knowledge. This solution features are derived from the questionnaire survey result analysis. The prevention and eradication for this system is defines as:

a. ***Prevention***: This procedure is to avoid and prevent the virus from the entire system completely.
b. ***Eradication***: This procedure is to remove the virus from the entire system completely.

The solution given in this system is based on the solution provided in antivirus advisories, computer viruses book and MyCERT advisories (www.mycert.org.my). The antivirus advisories are from the Symantec antivirus (www.symantec.com), Trend Micro antivirus (www.trendmicro.com) and F-Secure antivirus (www.f-secure.com).

The different type of virus controls the solution of the ECOVP system. There are three main types of viruses as shown in Figure 3. Boot sector infectors attach themselves to the boot sector of hard or floppy disks containing the computer’s start-up instructions. These viruses overwrite the original boot sector instructions so that they take immediate control. They tend to create bad sectors on the disk where they store the rest of their program code. System infectors attach themselves to various part of the computer’s operating system or master control program software. The virus may infect the input or output section of the operating system coding, the command interpreter or any other system file. They gain control of a system before virus detection or prevention program can get into the memory to do its job. Application infectors can affect any applications program. These viruses may or may not be memory resident and may infect every time a new program is loaded or a program is copied from one disk to another. These three main types of the virus are later categorized into eight types because this virus type will vary the solution of the system. The eight types are also shown in Figure 3.

Figure 3
Virus Type Structure

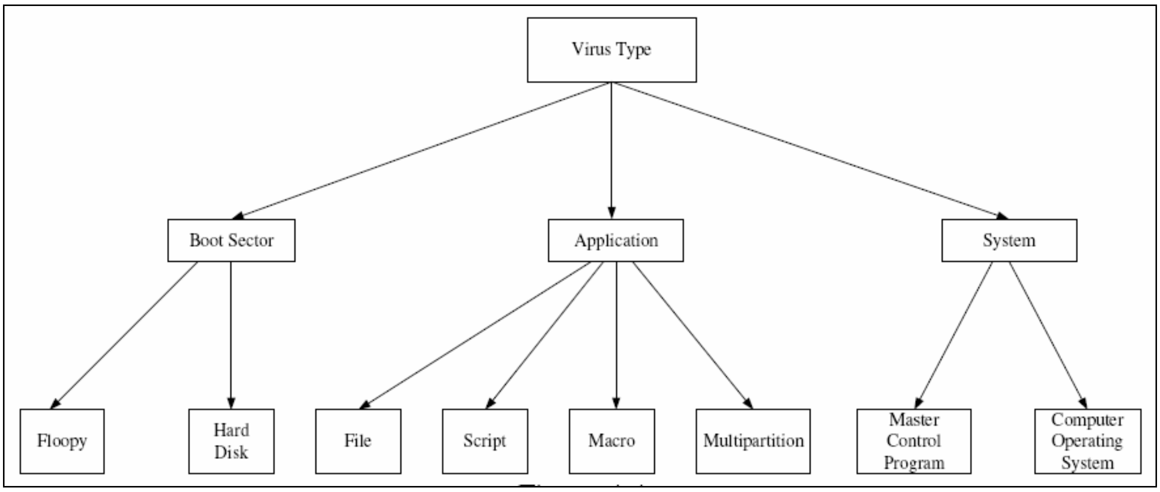


Table 1 shows example how the three different solutions are produced although the user selects the same symptom.

Table 1
Variety of Solution

Virus Type	Symptom	Solution
Boot Sector	Computer shutdown automatically	**Prevention**: Disable start boot up computer from external device. **Eradication**: Boot up from clean floppy disk.
Application	Computer shutdown automatically	**Prevention**: Disable the active scripting and the auto executable command. **Eradication**: Make sure to patch the application with the latest patch.
System	Computer shutdown automatically	**Prevention**: Always patch the OS with the latest patch by clicking

		the Windows Update. **Eradication**: Patch the OS with the latest patch.

6. Results

The questionnaire result and analysis provides the current situation of the computer viruses awareness, virus prevention levels in organizations and the damage computer viruses have caused in Klang Valley and Putrajaya. The result from the questionnaire survey showed that the users had a good knowledge related with the eradication procedure, antivirus functionalities and capabilities and used the information received related with viruses to equip themselves with the latest information of viruses, and they were prepared in confronting the viruses spread. The prevention level for organization was very good but users were not satisfied with the virus protection and viruses had a big impact to them where one of the major impacts was they were unable to perform their daily work. Even though the level of the user awareness and virus protection is very good, that does not mean the eradication and prevention procedure taken by the user are efficient and effective. Based on the questionnaire conducted also, most of the user interested to know the prevention and the eradication procedure when confronting the virus incident.

The ECOVP (Efficient Control of Virus Propagation) system is considered as capable to handle incident efficient and effectively when the end user is succeeded to clean up (eradicate) and do preventive measure to the infected machine. The ECOVP system is also capable to educate user about computer viruses and helps to control computer virus propagation. The users succeeded in identifying the seven main characteristics of the virus (the symptom, propagation mechanism, payload, virus type, operating algorithm, trigger mechanism and severity), which are used as the input to ECOVP system. The users also succeeded to clean up the virus in the infected machine based on solution given by the ECOVP system. The damages made by the viruses were succeeded cleaned by the user’s shows that the existence of the ECOVP system is important as supportive system to help user in ICT usage.

7. Conclusion

Nowadays, hundreds of different computer viruses are written every day, and their numbers are increasing rapidly. The results gathered from the questionnaire survey shows users in the sampling population have good knowledge about computer viruses and ready in confronting virus incidents. There still lack of research related with user education of computer viruses in Malaysia. This study could be one of the researches done to address this problem. The ECOVP system shows there is a need for developing efficient and effective system that has standard operating procedure in handling computer viruses incident.

References

Iman, M.R.M. “Negara Rugi RM31 Juta Serangan Terbaru Virus Komputer,” *Utusan Malaysia*, 29 August 2003, http://www.niser.org.my/news/2003_08_29_01.html.

Kephart, J., and White, S. “How Prevalent are Computer Viruses?”, http://www.research.ibm.com/antivirus/SciPapers/Kephart/DPMA92/dpma92.html.

“MA-041.052002: Computer Worm Incident Handling Standard Operating Procedure” *Malaysia Computer Emergency Response Team (MyCERT)*, 2 May 2002, http://www.mycert.org.my/advisory/MA-041.052002.html.

Perry, D. “The future of viruses,” *PC Answers*, Issue 108, July 2002, http://www.pcanswers.co.uk/tutorials/default.asp?pagetypeid=2&articleid=7929&subsectionid=607.

“SANS Glossary of Terms Used in Security and Intrusion Detection”, *SANS Institute*, May 2003, http://www.sans.org/resources/glossary.php#I.

Saudi, M.M. “Situational Report on Major Worms Outbreaks Up to Year 2003 in Malaysia,” 2004, http://www.mycert.org.my/other_resources/NISER-MYC-PAP-7070-1.pdf.

“The Reverse Challenge,” *The Honeynet Project*, http://www.honeynet.org/reverse/.