Knowledge Structure on Virus for User Education

Madihah Saudi[1] and Nazean Jomhari[2]

[1] Faculty Science and Technology,
Islamic Science University of Malaysia(USIM),
Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan, Malaysia
madihah@admin.kuim.edu.my
[2] Faculty of Computer Science & IT
University of Malaya
50603 Kuala Lumpur, Malaysia
nazean@um.edu.my

Abstract. There are many factors contribute to the virus spread and infection. One of the big challenges in confronting computer viruses is to educate user. It needs a lot of effort to educate user about computer virus. The researchers have produced ECOVP which is to help user handle virus problem and the targets users including home user, non-IT literature background and IT personnel needs in handling virus incident. Researchers had studied what are the information needs to be process, so we could use them to generate the knowledge on how to handle the virus problem. We had identified seven important criteria for user need to understand in capable for them facing the computer virus. However, this paper is focusing on virus attack on Windows platform only.

Keywords: virus, user education, symptom, propagation, mechanism trigger, payload, severity, operating algorithm, virus type.

1 Introduction

From Symantec website, worm is defines as program that replicate itself from system to system without the use of a host file. As for Trojan Horse it is refers as an impostors, files that claim to be something desirable but, in fact, are malicious[1]. Viruses are in contrast to worms, which require the spreading of an infected host file. A very important distinction between Trojan horse programs and viruses is that they do not replicate themselves. Trojan Horse contains malicious code that when triggered could caused loss, or even theft, of data. In order for a Trojan horse to spread, it is must for the Trojan horse program to be executed in the victim's host.

From the reference to [1], [2], [3], [4] and research made by the researchers, the differences between virus, worm and Trojan horse is summarized in the Table 1. As conclusion worm and virus are very similar to one another but are technically different in the way that they replicate and spread through a system. As for Trojan Horse its capability to control PC remotely makes it different from worm and the virus.

Y. Wang, Y. Cheung, and H. Liu (Eds.): CIS 2006, LNAI 4456, pp. 817–823, 2007.

Table 1. The Differences between Virus, Worm and Trojan Horse

Virus	Worm	Trojan Horse
Non self replicate	Self replicate	Non self replicate
Produce copies of themselves using host file as carriers	Do not produce copies of themselves using host file as carriers (independent program)	Do not produce copies of themselves using host file as carriers (independent program)
Cannot control PC remotely	Cannot control PC remotely	Can control PC remotely
Can be detected and deleted using antivirus	Can be detected and deleted using antivirus	Sometimes cannot be detected and deleted using antivirus

2 The Needs of User Education on Handling Computer Virus

User education is as important as anti-virus software. Training users in safe computing practices, such as not downloading and executing unknown programs from the Internet, would slow the spread of viruses [5].

Quoted from Symantec press release on September 27th 2004 at Cupertino, California[6], it stated that many employees in today's workforce are not aware that they play an important role in their organization's security. In other word, it is the lack of user awareness among the employees. According to META Group research, 75 percent of organizations identify a lack of user awareness as moderately or severely reducing the effectiveness of their current program. Additionally, 66 percent cite executive awareness as a concern.

Another survey conducted by the Chinese Ministry of Public Security shows that approximately 85 percent of computers in the country were infected with a virus on 2003. As one of initiatives, to help China to countermeasure this problem, Sophos the anti virus company is doing its part by sharing information about safe computing and how businesses can best protect themselves from virus attack[7]. Sophos is doing its part to increase user education about security threats in China.

Until today there are still many people click on email attachment from untrusted source. Who should be blamed? So, user needs guidance to avoid from being infected by the virus, worm, Trojan Horse or spyware.

3 Structuring Knowledge on Computer Virus

The domain knowledge of this project is the computer viruses on Windows platform. It is part of the malicious code. This domain knowledge consists of two main parts. So how can we classify the virus information? In order to retrieve important information related with the computer viruses for the usage of the ECOVP system, the structure of the computer viruses classification that was proposed by the researchers was used for the system.

There are thousands of variations of viruses, the classification of computer viruses[8] can be done via several ways which are based on the type of host victim, the type of infection technique and the special virus features. A common tripartite model of a computer virus structure consists of three parts [8]; Infection mechanism, Trigger and Payload. For this project, based on researcher observation and research, to ensure the system for this project is structured and easy to be implemented, using the Marko Helenius's as the basis concept in computer virus classification, the computer virus classification in this project is classified based on:

- The *Infection mechanisms.*
- The *Operating algorithm.*
- The *Payload*

Figure 1 is the computer viruses classification for this project. From this virus classification, later seven main features are extracted and the seven main features are verified and identified to be included as the problem descriptor for the proposed system.

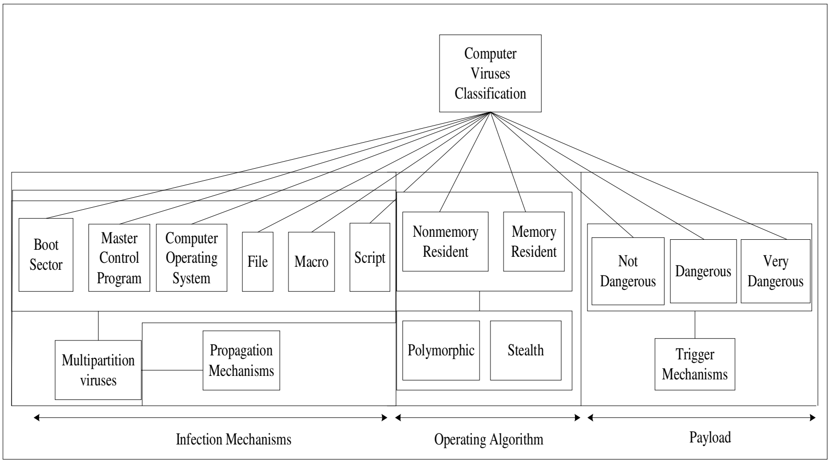


Fig. 1. Virus Classification for ECOVP System

Another form of classification of computer viruses [9] is based on the three ways a virus may add itself to host code as a shell, as an add-on and as an intrusive code. As for Marko Helenius[10], he classified computer viruses into four basic classes by infected objects. The computer viruses are classified into boot sector viruses, file viruses, macro viruses, script viruses and multipartition viruses.

This information was used by the researcher to ensure the system is capable to produce the required solution. The infection mechanisms, operating algorithm and payload can be divided into more specific parts in order to fulfill user needs.

The whole virus classification diagram for ECOVP system was illustrated in Figure 1 while the input and output process illustrated in Figure 2. The information virus classification is sub categorize into seven main features which are used as the input or also known as the problem from the user. The seven features are symptom, propagation, trigger mechanism, payload, severity, operating algorithm and virus type. How do we derived these seven important criteria in ECOVP was explained in Figure 3.

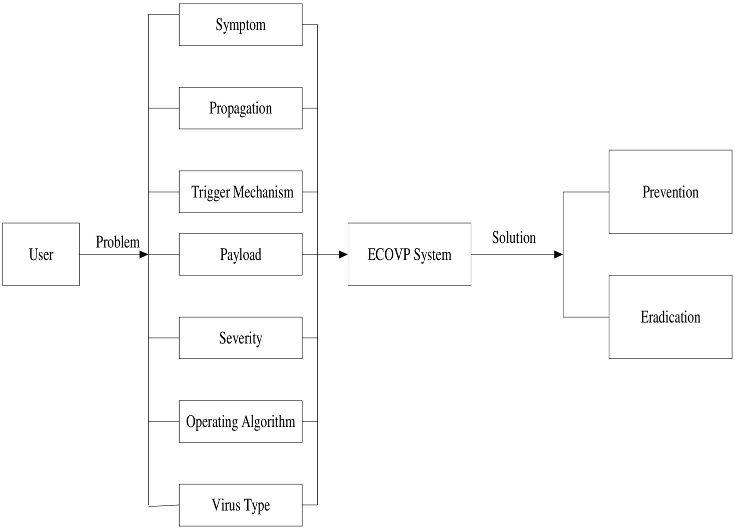


Fig. 2. Input problem and output solution

The problem which is the input from user, contributes to variety of solution where the solution consists of the prevention and eradication procedure. The input from a user which is also known as the problem consists of symptom, propagation, mechanism trigger, payload, severity, operating algorithm and virus type.

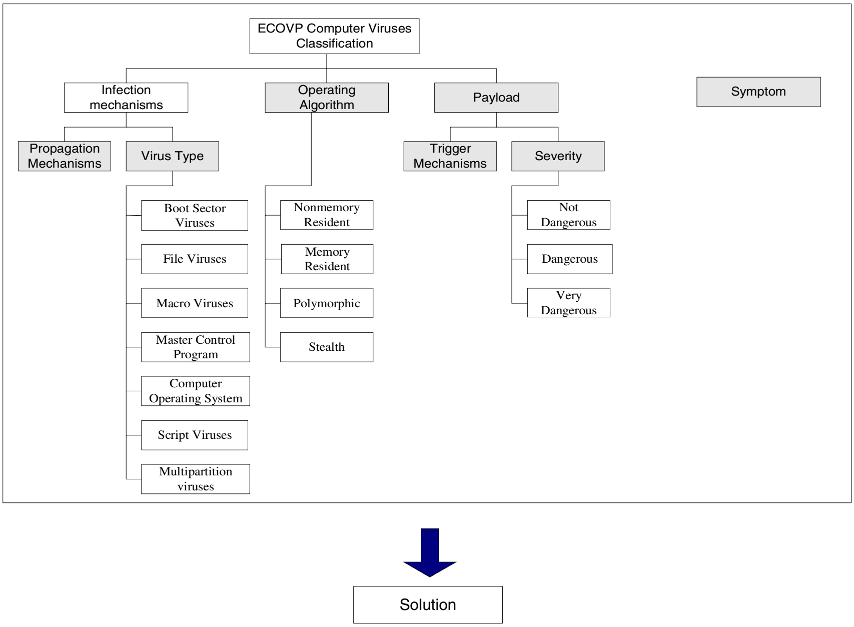


Fig. 3. Problem derivation features

The problem features stated above are derived from the virus classification. For each of the main features it consists of the infection mechanisms, operating algorithm and payload can be divided into more specific parts as illustrated in Figure 3. The highlighted was the main features that user have to key in the data into the system to get the eradication and prevention solution.

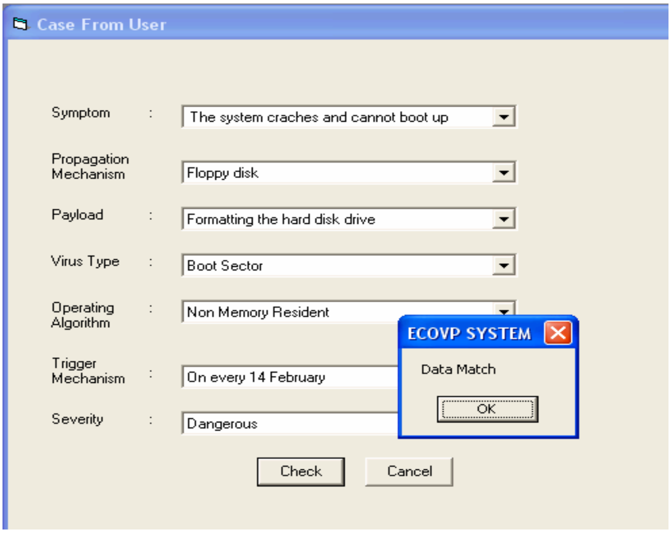
Referring to Figure 3, below is the details explanation of the figure:

- The top box which consists of the ECOVP computer viruses classification is the computer virus classification made by the researchers which was extracted from Figure 1, while Figure 2 summarized the computer viruses classification for ECOVP system. From the ECOVP computer viruses classification, six main features that are used for the ECOVP system are extracted.
- The ECOVP Computer Viruses Classification is categorized based on three main categories which are the infection mechanisms, operating algorithm and payload. Each of these main categories has its own feature. Then these three main categories are extracted and are put in the middle box.
- In the middle box, from these three main categories, for infection mechanisms, it is subcategorized into two categories which are the virus type and propagation mechanisms. These two categories contribute as the main features in the ECOVP system. The virus type consists of boot sector viruses, file viruses, macro viruses, master control program, computer operating system and multipartition viruses features.
- The operating algorithm is extracted as one of the main feature for ECOVP system. The operating algorithm consists of nonmemory resident, memory resident, polymorphic and stealth.
- As for the payload, it is subcategorized into severity and trigger mechanisms which contribute as the main features for ECOVP system. The severity consists of non dangerous, dangerous and very dangerous features. Even though the payload has been subcategorized, still the payload is chosen as one of the main feature in the ECOVP system due of its importance roles in identifying the solution.
- Another feature that is included as the problem descriptor is the symptom of the viruses. The symptom is not derived from the ECOVP computer viruses classification. It is chosen as one of the main features because it is one of the main important features needs to be identified by the user as the problem descriptor of the system.
- From these seven main features the solution which consists of the prevention and eradication is derived. These seven main features play important role to determine the solution that will be displayed to user.

4 Solution

A solution consists of the prevention procedure and eradication procedure. As illustrated in Figure 5, the solution is consists of the prevention and eradication procedure. The solution is also part of the domain knowledge. Based on the questionnaire conducted, most of the user interested to know the prevention and the eradication procedure when confronting the virus incident. 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.


Case From User

Symptom : The system craches and cannot boot up

Propagation Mechanism : Floppy disk

Payload : Formatting the hard disk drive

Virus Type : Boot Sector

Operating Algorithm : Non Memory Resident

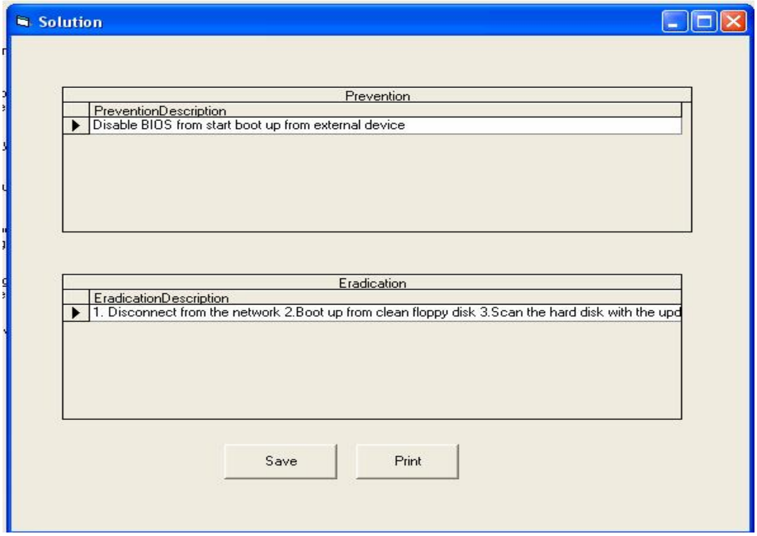
Trigger Mechanism : On every 14 February

Severity : Dangerous

ECOVP SYSTEM

Data Match

Fig. 4. Match Search


Solution

Prevention

PreventionDescription
Disable BIOS from start boot up from external device

Eradication

EradicationDescription
1. Disconnect from the network 2.Boot up from clean floppy disk 3.Scan the hard disk with the upd

Fig. 5. Match Solution

The solution given in this system is based on the solution provided in anti virus advisories, computer viruses book and MyCERT advisories. The anti virus advisories are from the Symantec anti virus, Trend Micro antivirus and F-Secure anti virus.

5 Conclusion

The derivation of the seven important elements was based on Marko Helenius who is the experts on virus. The seven features are symptom, propagation, mechanism trigger, payload, severity, operating algorithm and virus type. This information is very important in identifying the eradication and prevention solution in handling virus. If user could not understand the term, this system is capable to offer support if user wants to know more detailed on contextual information on each term by moving the mouse to the label of the problem descriptor and the explanation of each label is displayed. Hope this system would help computer user in handling virus especially on Windows platform.

References

1. Symantec.: What is the difference between viruses, worms, and Trojans? (1999) [Online]. Available: http://service1.symantec.com/SUPPORT/nav.nsf/docid/1999041209131106
2. Saudi, M.: Combating Worms Outbreaks: Malaysia Experience (Common Ground). International Journal of Learning (Common Ground) 12(2), 295–304 (2006)
3. Resnet.: The Difference Between a Trojan Horse, Virus and a Worm. (2004). [Online]. Available: http://www.lasalle.edu/admin/it/portal/virus_updates/trojan_horse_virus_worm.htm
4. Microsoft: What is a virus, worm, or Trojan Horse? (May 23, 2005) [Online]. Available: http://www.microsoft.com/athome/security/viruses/intro_viruses_what.mspx
5. Antivirus.world.com.: How Does Anti-Virus Software Work? (August 23, 2005) [Online]. Available: http://www.antivirusworld.com/articles/antivirus.php
6. Symantec: Symantec Education Services Program Emphasizes Employee Training for Improved Security Posture (September 27, 2004) [Online]. Available: http://www.symantec.com/press/2004/n040927.html
7. Sophos.: China Crisis: Computer Viruses Rampant Says Survey. (October 21, 2003) [Online]. Available: http://www.sophos.com/virusinfo/articles/chinavirus.html
8. Martin, R.: FAQ der VIRUS.GER: Version 2.3. (1997) [Online]. Available: http://www.virushelpmunich.de/faq/faq
9. Spafford, E.H.: Computer Viruses as Artificial Life. Artificial Life 1(3), 249–265 (1994)
10. Helenius, M.: A System to Support the Analysis of Antivirus Products' Virus Detection Capabilities. PhD Dissertation, Department of Computer and Information Sciences, University of Tampere (2002)