Virus Combat: Promoting Awareness on Viruses Through Video Game

Dahlan Abdul Ghani, Rafiqi Izani Faiz bin Redzuan

Abstract— Technology nowadays are vastly growing and by that the number of virus are also increasing each day. There were 60,000 known viruses, Trojans, worms, and variations and today there are well over 100,000 known computer viruses. In addition, studies and researches show that a computer connected to the Internet may experience an attack every 39 seconds. The purpose of this research is promote the importance of computer viruses using computer game platform. In Malaysia, there are still less effort of using new media on preventing computer virus and Malaysian society are still lacking of knowledge and awareness on how to avoid their computer from getting occurrence or harmed by virus. Furthermore, this research will also assess the efficiency of the 3D game prototype among selected respondents.

Keyword: technology; computer virus; video game; program; Internet.

I. INTRODUCTION

A computer virus is a program that is designed to damage or disrupt the normal functions of your computer and its files. Like biological viruses, computer viruses attach themselves to a host, usually a program file, data file, or a file in your computer's operating system. From here, it replicates itself, spreading the infection to other files. The word “Computer virus” was described formally by Fred Cohen back in 1983, while he was at the Digital Equipment Corporation VAX systems performing academic experiments” (Dwan, 2000). The virus writers released a virus called Whale, which was a self-modifying virus in 1990. Then, GPI virus was discovered in 1991, the virus objective was to steal Novell NetWare passwordswhich at the same year Michelangelo was spotted in New Zealand, according to Dwan (2000). A new technique was uncover to cope with the communication revelation and internet popularity, “The first reported macro virus ‘Concept’, was seen in the wild by AV researcher Sarah Gordon in summertime of 1995. A set of five macros designed only to replicate, Concept’s payload displays the virus author’s ominous message: ‘That’s enough to prove my point’ ”. (Paquette,2000)

Ever since, a new age began to develop. Macro viruses were getting attention each year. Dubbed 'XM.Laroux' was brought to life in 1996 while Melissa was able to taint millions of computer and approximately causes $80m damages in March 1999. It was an email consist of an infected file attachment addressed as essential message from known people. (News.bbc.co.uk, 2002). Chermobyl strain CIH affecting approximately 540,000 computers in Turkey and South Korea a month later. The objective was to reset the hard drive and zap a key chip on the motherboard. (Dwan, 2000).

In 2000, a new Millennium era had just began. Apparently, the virus writers is full of surprises. It was a message consist of a love letter "Love Bug". The only thing the user have to do is to affect his system and send copies of viruses automatically to anyone in his e-mail contacts to open the file attachment (Ruppe, 2000). The virus had cause catastrophe and damage to computers throughout the world (Ruppe, 2000). Pentagon and White House were forced to temporaryly stop the public access to their web in 2001 and 250,000 systems were affected due to "Code Red" worm in nine hours, which was able to crack hundreds of thousands of computers after the first clarification on July 19th (Stenger, 2001).

Though, malware or malicious ware began releasing viruses regardless of the writers objectives to write the virus. As software developers began to realize the necessary for developing applications to defend computers from bugs and viruses, the malware began between writers for the virus and antivirus companies. Each primary intention of a direct action virus is replication and to spread infection whenever the code is executed. When certain conditions have been met, the virus is set into action and begins to infect files in the directory or folder it's located in. It also infects those in directories attached with the AUTOEXEC.BAT file path. This extension represents a batch file which is always found in the root directory of your hard drive, responsible for performing certain operations when the computer is booted up.

Spyware that is installed for innocuous reasons is sometimes referred to as tracking software. It runs quietly in the background, collecting information or monitoring your activities to trigger malicious activities related to your computer and how you use it. That includes capturing keystrokes, screen shots, personal email addresses, Internet usage information, and other personal information, such as credit card numbers.The virus usually finding its way onto computer without user’s knowledge or permission, attaching itself to your operating system, maintaining a presence on user’s PC.

File Allocation Table or also known as FAT, is a mechanism hired by Microsoft and used in most Windows

Revised Manuscript Received on September 10, 2019.

Dahlan Abdul Ghani, Universiti Kuala Lumpur, Malaysian Institute of Information Technology 1016, Jalan Sultan Ismail, 50250 Kuala Lumpur (E-mail: dahlan@unikl.edu.my)

Rafiqi Izani Faiz bin Redzuan, Universiti Kuala Lumpur, Malaysian Institute of Information Technology 1016, Jalan Sultan Ismail, 50250 Kuala Lumpur. (E-mail: izani2295@gmail.com)

operating systems. The task is to keep pathway of all the substances on a disk. The FAT is basically a chart which contains numbers that correspond to cluster addresses on a hard drive. The common danger to the File Allocation Table(FAT) is the relation to each virus. Instead of inserting a malicious code directly into infected files, it distributes itself by manipulating the method in which files are accessed by the FAT file system. Once an infected file is executed, a link virus typically creeps into resident memory and writes a hidden file to the disk. Trojan Horse computer virus, are mostly not able to replicate itself, nor can it propagate without an end user's assistance. Therefore, the assailants essential use social engineering tactics to trick the end user into executing the Trojan. Identically, the malware programming is hidden in an innocent-looking email attachment or free download. Every time the user clicks on the email attachment or downloads the free program, the malware mostly are buried inside is transferred to the user's computing device. Once inside, the malicious code can execute whatever task the attacker designed it to carry out.

A type of computer virus that will copy its own code over the host computer system's file data, which destroys the original program. The virus has affected a wide range of operating system including Windows, DOS, Macintosh and Linux. The only way to infect a computer with a file infecting virus is to execute an infected file on the computer. The infected file may come from a multitude of sources including: floppy diskettes, downloads through an online service, network, etc. Once the infected file is executed, the virus may activate. It deletes the data (partially or completely) and replace the old code with their own. They replace file/program content without changing its size.

2.3 Results & Discussions

2.3.1 Game Design : Virus Attack

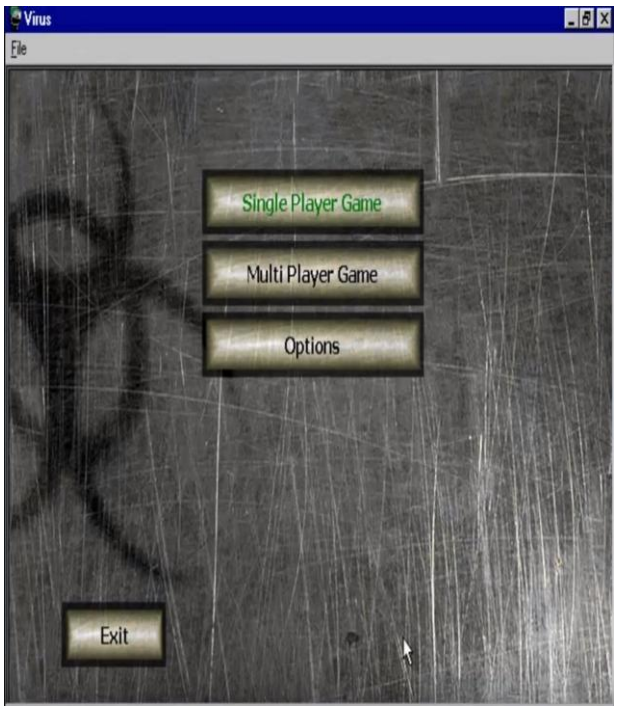

Figure 1.0: Interface of Virus: The Game

Figure 1.1: Gameplay of Virus: The Game

Game user interface (UI) were too outdated aimed at today's game design and interface standard and certainly need more simplify and neatly arrange icons and buttons (see Figure 1.0). Moreover, the game interface should be more straightforward and user-friendly with smooth animation and graphics for better user experience. The visual quality of a game is very important; it is hard to sell a game if it looks bad, even if the game-play is fun. (Brent Fox, 2005).The role of a good UI is to provide relevant information clearly and quickly, and to get out of the way once it has done its job(Desi Quintans, 2013).

The UI interface are located at bottom down of the screen main page (see Figure 1.1), it makes the game interface looks crowded with very less breathing space for the user to navigate around and make the user feels uncomfortable for a long period of time when playing.

Game design is the act of deciding what a game should be. That's it. On the surface, it sounds too simple (Jesse Schell, 2008).

2.3.2 Virus Resurrection

Figure 1.2: Virus Resurrection

According to Richard Rouse (2005), the game design determines what choices players will be able to make in the game-world and what ramifications those choices will have on the rest of the game. This game is a great example of a good indie style game. The whole experience in the game was resembled using the Windows 98 Operating System environment. The gameplay is great where player must control an antivirus fighting each well-known virus in a "boss fight" like scene. However, the downside of the user experience is that the player can't control the movement of the antivirus (main character), but the user can use the main character auto movement to timely shoot the enemy.

A good shooting game should be able to fully control the character movement in the game in order to give realistic feeling during the combat. According to Jyrki Turunen (2017), combat is about efficiency, about predicting your opponent and calculating the best chances of successfully winning that particular scuffle.

II. WATERFALL MODEL

Waterfall model is the most common model use by game developers to develop basic game environment. It helps to define tasks that must be handled during the development process of each phase. Figure 1.2 shows six phases in Waterfall model.

According to Youssef Bassil (2012), the Waterfall model which comprises six stages to be completed consecutively in order to develop a software solution. Waterfall model has being proven successful through many software development firms and industrial manufacturers have implemented it as their prime development charter/pipeline and SDLC to plan, build, and maintain the products. Additionally, the firms went to the extreme by establishing several departments each of which is run by a team of expert people totally responsible for and dedicated to handle a particular phase of the Waterfall model. This includes, for instance, business and requirements analysis department, software engineering department, development and programming department, quality assurance department, and technical support department.

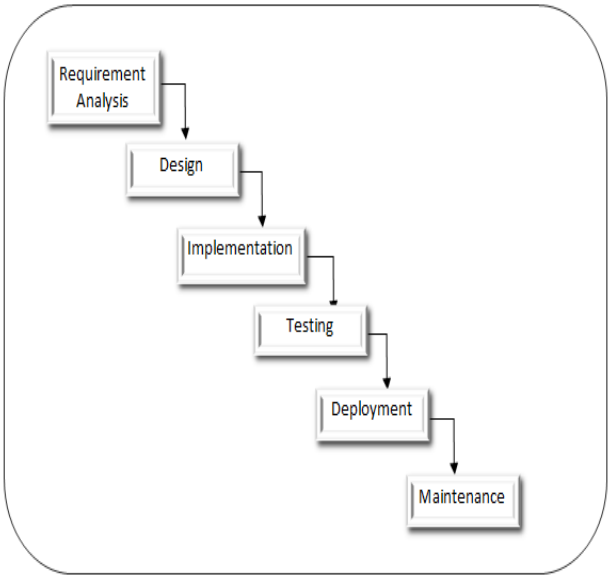

Figure 1.2 Waterfall Model

Figure 1.2 shows that framework of Waterfall model. There are six phases to complete the project phases.

3.1 Requirement Analysis

During this initial phase, the potential requirements of the application are methodically analyzed and written down. The activities during this phase includes finding the problem statement on computer virus, studying on what the game needs, searching games that is related to the topic and usage of a suitable software and programs for the project. The researcher will give a set of 25 questionnaire to the target audients and the data result is typically a requirements document that defines what the application should do, but not how it should do it. The data were entered into the computer using SPSS software. Results were presented through frequency counts and other descriptive statistics. The data were transcribed.

3.2 Data Analysis Approach

This research utilized the quantitative research methodology. The instruments used to collect the data were questionnaire. A set of questionnaires containing 50 questions divided into 6 sections was developed based on a questionnaire used previously by another study (Gerber & Green, 1999). Different question-types, such as ranking, yes-no, listing, category, open-ended and scales were used in questionnaire. The questionnaire was piloted to group of 25 students to access its validity before it was distributed. To analyze the data, data were entered into the computer using SPSS software. Results were presented through frequency counts and other descriptive statistics. The data were transcribed.

REFERENCES

1. Dwan, B. (2000). The Computer Virus - From there to here. In B. Dwan, *Computer Fraud and Security* (pp. 13-16).
2. Fox, B. (2005). *Game Interface.* Boston: Thomson Course Technology PTR.
3. Jigyasa sengar, Harshita chawla. (2017). Research Paper On Computer Virus :A Survey. *GADL Journal of Inventions in Computer Science and Communication Technology (JICSCT)*, 1-4.
4. Kai Peterson. (2009). The Waterfall Model in Large-Scale Development. Sweden. Retrieved from http://www.diva-portal.org/smash/get/diva2:835760/FULLTEXT02.pdf
5. *Melissa virus creator jailed*. (2002, May 2). Retrieved from news.bbc.co.uk: http://news.bbc.co.uk/2/hi/americas/1963371.stm
6. Quintans, D. (2013, January 22). *Game UI By Example: A Crash Course in the Good and the Bad*. Retrieved from gamedevelopment.tutplus.com: https://gamedevelopment.tutsplus.com/tutorials/game-ui-by-example-a-crash-course-in-the-good-and-the-bad--gamedev-3943
7. Rouse, R. (2005). *Game Design: Theory & Practice.* Plano: Wordware Publishing, Inc.
8. Ruppe, D. (2002). *"'Love Bug' Travels the Globe"*. Retrieved from abcnews.go.com: http://abcnews.go.com/1/sections/world/Daily

News/Lovebug000503_world.html
9. Schell, J. (2008). *The Art of Game Design: A Book of Lenses*. Burlington: Elsevier Inc.
10. Stenger, R. (2001, July 31). *Net braces for stronger 'Code Red' attack*. Retrieved from edition.cnn.com: http://edition.cnn.com/2001/TECH/internet/07/30/code.red/
11. Turunen, J. (2017). *The Good, The Bad and The Unpleasant - A Study of Graphical User Interface in Video Games*. Tampere: Tampere University of Technology.
12. Youssef Bassil. (2012)." *A Simulation Model for the Waterfall Software Development Life "* Lebanon: International Journal of Engineering & Technology (iJET).