COMPARISON OF TWO METHODS FILE NAME SCANNING AND STRING SCANNING ON COMPUTER WORM DETECTION

Mario Florentino Makang

Jurusan Teknik Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Komputer Indonrsia
Jln. Dipati Ukur No.112 Bandung 40132
marioflorentinomakang@yahoo.co.id

ABSTRACT

The many types of malware (malicious software) that are on the computer and the impact of malware is very harmful for the computer user. One type of malware is a worm.

Like other malware or Trojan viruses and the like, the worm has a destructive force that can be very good for injure personal users and users in a large capacity (up to the internet network).

To overcome this there are two methods that can be done to detect the presence of a computer worm. The scan method File Name Scanning and String Scanning. Where the first method oriented to the name of a file-oriented and the second row in the hex string to the detection (scan) on a worm file.

The purpose of this final task is to implement both methods, and also to test with some test parameters, to determine which method is more optimal detection of doing the worm file.

Tools used to build this application is MS. VB 6.0. Helper tools used is HxDen (decimal hex editor).

Results to be achieved from this aplication is only to be able to detect the worm files which will be tested is to know thye time and accuracy in detecting the worm file.

This application has been successfully tested two methods above. In addition to detecting the presence of the worm files, can also be advantages and disadvantages of the test parameters. So that could be useful to the user in performing the detection and also can find out where the best method or the same between the two methods.

Keywords : *File Name Scanning*, *String Scanning*.

1. INTRODUCTION

1.1 Latar Belakang

Computers are machines whose development over time has progressed very rapidly. The function of the computer itself is to process the data, where data here is something that does not have meaning for the recipient and still requires the existence of a treatment. Data can form a state, images, sounds, letters, numbers, language or other symbols that we can use as an ingredient to view a situation.

Information processing is the result of a model, formation, organization, or a change in the form of data that has a particular value, and can be used to increase the knowledge of the accepted. In this case, the data can be considered as an object and information is a subject that will benefit the recipient. Information can also be called as a result of processing or data processing.

So that we can see that the main function of a computer is processing the data mentioned above into a useful information or useful to recipients.

But in computer development can not be separated from a crime against a computer program. One of the crimes in the worm program. Computer worm can cause a very serious impact and harm. An example of a slow computer, disk drive accessible on a regular basis, changing the computer configuration and so forth.

Based on the above, to anticipate developments and the increasing number of worms, then needed a program that can detect and remove malicious programs that. and the comparison between both methods.

1.2 Problem Identification

How to build **COMPARISON OF TWO METHODS FILE NAME SCANNING AND STRING SCANNING ON COMPUTER WORM DETECTION**.

1.3 Objectives

From the background described the writer intended to build application programs Application Development detection Computer Worm With File Name Scanning Method And String Scanning.

While objectives to be achieved in this research are:

1. Implement methods Scanning and File Name String Scanning in the application file infector removal.
2. Detecting file infector worm on the computer.
3. Deleting a file infector worm from your computer system.
4. Knowing performance based on the time taken by each method.
5. Knowing the accuracy of each method in terms of the worm file search.
6. Can find out which method both in terms of time and worms file search results.

1.4 Benefits

The benefits of this application development include:

1 Detecting file infector worm on the computer.

2 Delete the file infector worm from your computer system.

3 Knowing performance based on the time taken by each method.

4 Knowing the accuracy of each method in terms of the worm file search.

5. Where can find a good method in terms of time and worms file search results.

2. MODEL, ANALYSIS, DESIGN AND IMPLEMENTATION

2.1 Model

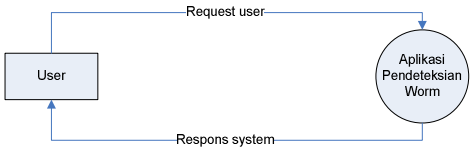
1. Data collection phase
   a. Studies Library.
   b. Observation.
2. Stage of software creation.
   a. *Requirements analysis and definition*
   b. *System and software design*
   c. *Implementation and unit testing*
   d. *Integration and system testing*
   e. *Operation and maintenance*

2.2 Analisis Masalah

Analysis system can be defined as the decomposition of a complete information system into its component parts to identify the problems and obstacles that can be proposed to the needs repairs. Analysis phase is the most critical stage and is very important, because errors in this stage will cause an error also in the next stage. Analysis of this system are obtained through the observation will be found some data and facts that will be used as test material and the analysis to the application and development of an application of the proposed system.

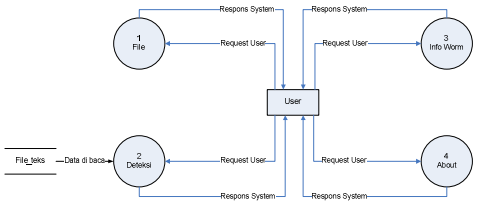
2.3 Design

1. Diagram Konteks



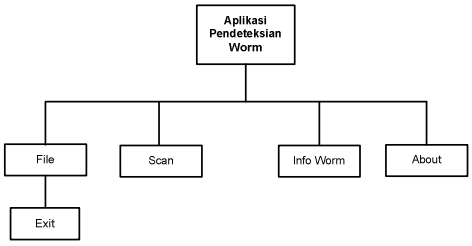
Picture 3.7 Diagram Konteks Aplikasi Pendeteksian *Worm*

2. DFD Level 0



Picture 3.8 DFD Level 0

3. Struktur Menu



Picture 3.15 Struktur Menu Aplikasi

2.4 Implementasi

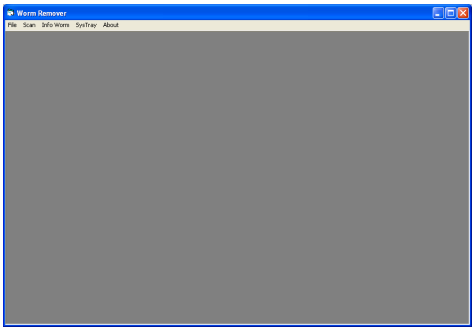
The software used on computer systems used to build applications on the computer worm detection is as follows:

1. Operating System Windows XP Professional SP 2.
2. *Visual Basic* 6.0.

Minimum requirements for hardware (hardware) needed to implement programs created application is a PC computer hardware is compatible with the specifications mentioned below.

Minimum needs are:

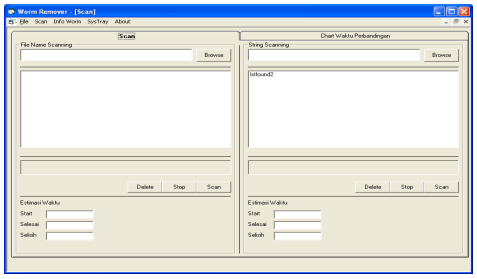
1. Processor : CPU Minimum 1.0 GHZ
2. Memory : Minimum 512MB RAM
3. Hardisk : Minimum 20 GB
4. VGA : Minimum 32 MB



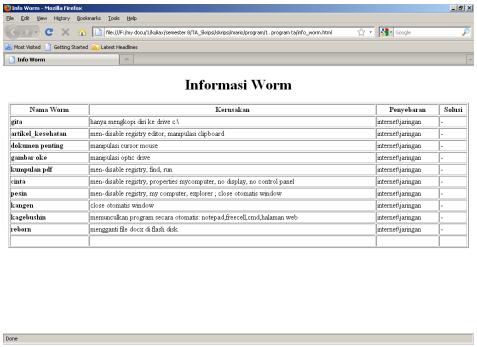
Picture 4.1 Tampilan Menu Awal



Picture 4.2 Tampilan Sub Menu File



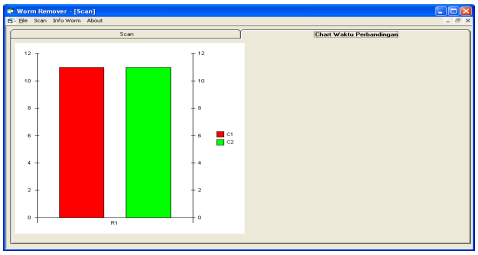
Picture 4.3 Tampilan Menu Scan



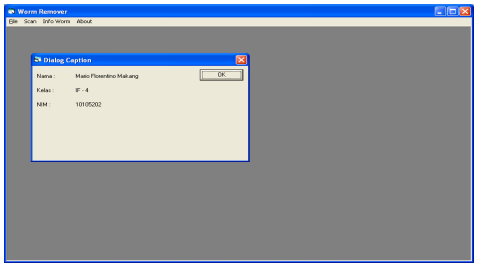
Informasi Worm

Nama Worm	Kemunculan	Penyebaran	Solusi
gita	hanya mengkopi dari ke drive c:\	internet/jaringan	-
artikel_kesehatan	non-disable registry editor, manipulasi clipboard	internet/jaringan	-
dokumen penting	manipulasi cursor mouse	internet/jaringan	-
gambar oke	manipulasi optic drive	internet/jaringan	-
kumpulan pdf	non-disable registry, find, run	internet/jaringan	-
cinta	non-disable registry, properties mycomputer, no display, no control panel	internet/jaringan	-
pesin	non-disable registry, my computer, explorer ; close otomatis window	internet/jaringan	-
kangen	close otomatis window	internet/jaringan	-
kapeluchin	menonaktifkan program secara otomatis: notepad,freecell,cmd,halaman web	internet/jaringan	-
reborn	menggantti file .docx di flash disk	internet/jaringan	-

Picture 4.4 Tampilan Menu Info Worm



Picture 4.5 Tampilan Sub Menu Chart



Picture 4.6 Tampilan Menu About

3. RESULTS AND DISCUSSION

3.1 Facilities Applications

Applications are built has the following capabilities:

1. Applying the two methods of scanning the file name and string scanning.

2. Can detect the presence of worms in a computer system (known worm).

3. Can remove detected worm.

4. Knowing the performance of each method with the parameters of time and accuracy of detection.

3.2 Software

This application will run normally on the software specification as follows:

a. Sistem Operasi Windows

4. CONCLUSION AND SUGGESTIONS

4.1 CONCLUSION

1. This worm detection applications built has implemented two methods of Scanning and File Name String Scanning in the application file infector removal.
2. This worm detection applications using two methods of Scanning and File Name String Scanning in the application file infector removal has identified the worm file on the computer system.
3. This worm detection applications using two methods of Scanning and File Name String Scanning in the application file infector removal has been able to delete the worm file on the computer system.
4. Comparisons are made to the two methods shows that both methods have the same detection time and accuracy of each method is the same.

4.2 SUGGESTIONS

1. Used scanning technology allows for the detection of worms on the computer system by anyone. Therefore, security issues must be kept in mind for the system to stay awake from other parties who are not interested, especially the security of this detection applications.
2. Programs that have built applications can only detect known worms.
3. Test data for both methods were very minimal. So highly recommended to develop test data better.

5. REFERENCES

[1]. Achmad Dharmal, (2006), *Computer Worm 1*, Jasakom, Jakarta.

[2]. Achmad Dharmal, (2006), *Computer Worm 2*, Jasakom, Jakarta.

[3]. Ilham Perdana, (2008), Petunjuk Penulisan Ilmiah, Perumusan Masalah, Pengumpulan Data Penelitian, Petunjuk Tata Tulis Ilmiah, *Handout Metodologi Penelitian*.

[4]. Wikipedia. (03 May 2009), *Visual Basic 6.0*, www.wikipedia.org/id

[5]. Wikipedia. (03 May 2009), *BASIC*, www.wikipedia.org/id

[6]. Indoskripsi. (03 May 2009), *Worms*, www.indoskripsi.com

[7]. Vbtutor. (03 May 2009), *Visual Basic 6.0*, www.vbtutor.net

[8]. Vb-bego. (03 May 2009), *Visual Basic 6.0*, www.vb-bego.com