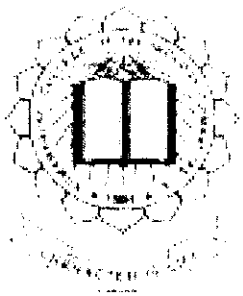


ANTIVIRUS WITH SPECIFIC REFERENCE FOR BAGEL WORM AND MYDOOMNOARG VIRUS

By

S.RAJESHKUMAR
(Reg. No: 71203621040)

Of

KUMARAGURU COLLEGE OF TECHNOLOGY
COIMBATORE

A PROJECT REPORT

Submitted to the

FACULTY OF INFORMATION AND COMMUNICATION ENGINEERING

In partial fulfillment of the requirements
For the award of the degree
Of

MASTER OF COMPUTER APPLICATION

June, 2006

KUMARAGURU COLLEGE OF TECHNOLOGY

COIMBATORE-641023

Department of Computer Science

Bonafide Certificate

Certified that this project report titled **ANTI VIRUS WITH SPECIFIC REFERENCE FOR BAGEL WORM AND MYDOOMNOAVG VIRUS** is the bonafide work of Mr.**S.RAJESHKUMAR** who carried out the research under my supervision. Certified further that to the best of my knowledge the work reported here in does not form part of any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

C. Rajan Kumar

PROJECT GUIDE

HEAD OF THE DEPARTMENT

Submitted for the University Examination held on 29-06-2006

29/6

INTERNAL EXAMINER

29/6

EXTERNAL EXAMINER

New # 77/2, Old # 26/2, Habibullah Road, T.Nagar, Chennai - 600 0
Voice : +91- 44 - 2822 7223, 2822 7224, 2822 7225
E-mail : aadhityaa@sancharnet.in, info@aadhityaa.com
URL : www.aadhityaa.com

AAD/PR/9789/05-06

To
Head Of The Department
Department of M.C.A.,
KUMARAGURU COLLEGE OF TECHNOLOGY,
Coimbatore.

Sir/Madam

Sub: **Project Completion**

This is to say that **Mr. S.RAJESH KUMAR** of **M.C.A., KUMARAGURU COLLEGE OF TECHNOLOGY**, have successfully completed her final year project entitled **"ANTIVIRUS WITH SPECIFIC REFERENCE FOR BAGEL WORM AND MYDOOMNOAVG VIRUS"** during the period **December 2005 to April 2006** in our company.

For Aadhityaa infomedia Solutions,

Administration-Manager.

CHENNAI-17

ABSTRACT

A (computer) virus is a program (a block of executable code) which attaches itself to, overwrites or otherwise replaces another program in order to reproduce itself without the knowledge of the PC user. Most viruses are comparatively harmless, and may be present for years with no noticeable effect: some, however, may cause random damage to data files (sometimes insidiously, over a long period) or attempt to destroy files and disks. Others cause unintended damage. Even benign viruses (apparently non-destructive viruses) cause significant damage by occupying disk space and/or main memory, by using up CPU processing time, and by the time and expense wasted in detecting and removing them.

This project connotes to an anti virus program which is capable of removing the Bagle Worm & Mydoomnovarg type of virus. This project checks for the virus signature if it matches that will be removed.

Bagle Worm :

Bagle is a mass-mailing worm that was found on 18th of January, 2004. The worm sends messages with the subject 'Hi' and random EXE attachment names. The worm installs a backdoor to infected machines. Bagle has been programmed to stop spreading on 28th of January.

Normally, Bagle variants search local hard drives of infected machines to harvest e-mail addresses, but Hyponnen said the new variants connect to a Web back-end server capable of generating unique e-mail addresses.

"Bagle may have fooled us into initially thinking that it was all about getting attention, but it quickly became apparent that this was professional software, where the author was adding and disabling different functions," said Gordon. "It's really the first time a virus writer was paying attention to the details, essentially following the CMMI process." This worm runs on Windows 95, 98, ME, NT, 2000 and XP.

MydoomNovarg:

A new virus which can be spread by ZIP. email attachments has been reported. These may get through our email virus ... W32.MyDoom is a rapidly spreading mass-mailing worm that uses its own SMTP engine to email itself to addresses harvested from infected systems, and installs a backdoor on infected systems on TCP port 1034. View this web cast to learn new information about this threat, as well as mitigating strategies and security solutions to prevent this worm from infecting your systems and to improve the overall security posture.

This worm sends email to addresses gathered from files with certain extensions, adding itself as an attachment. It uses Simple Mail Transfer Protocol (SMTP) to send out email with the following details:

ACKNOWLEDGEMENT

I wish to express my sincere thanks to **Dr. Joshep v.Thanikal** principal, Kumaraguru College of Technology, Coimbatore, for permitting me to undertake this project.

My deepest acknowledgement to **Dr. S. Thangasamy** Dean and **Dr.Gururajan** Head Of The Department, Computer Application and Engineering, Kumaraguru College of Technology, Coimbatore, for his timely help and guidance throughout this project.

I am greatly indebted to my guide **Mr. A. Muthukumar** Assistant Professor, Department of Computer Application and Engineering, Kumaraguru College of Technology, for his valuable guidance and encouragement at every stage of this project work.

I express my gratitude my project Coordinator **Mrs. V.Geetha** Assistant Professor,Department of Computer Application and Engineering, Kumaraguru College of Technology, who has been my guide with valuable and timely suggestions and extended kind of operation and encouragement.

I wish to thank my guide **Mr.C.RAJAN KRUPA** Senior Lecture and all my staff members for their timely help and guidance to complete the project successfully.

I express my sincere thanks to **Mr.Rajan**, Managing Director, **AADHITIYA INFOMEDIA SOLUTION, Chennai** for giving me the opportunity to do the project work in their concern. My deepest acknowledgement to **Mr.vaithilingam** Project Manager's AADHITIYA INFOMEDIA SOLUTION, for his support and assistance at various levels of my project work.

Finally, my heartfelt thanks to almighty god for helping me throughout the course of this project work.

TABLE OF CONTENTS

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 ORGANISATION PROFILE

AADHITIYA INFOMEDIA SOLUTIONS is a ONE STOP SOLUTION PROVIDER in the field of Information Technology providing quality solutions in areas of Local Area Networking, Wide Area Networking, software development and implementation and systems integration, data capture solutions, web based and multimedia solutions. Established in 2000.

Landmark InfoTech commenced operations with the setting up of a software training division and software development centre in India with the first centre at Chennai and also offers a total end to solutions in Networking, System Integration & implementation, Automatic data capture systems and Biometric solutions.

Aadhitiya Infomedia Solutions is a part of the 25 years old Landmark Group, which operates large Marketing Management in various parts of the world .Landmark group give important to the Customers and non-customers.

Landmark Group has been operating large financial companies in various parts of the world and predominantly in the Middle East. Landmark Group has ambitious global expansion plans and is gearing up to be one of the large Insurance groups in the world. The Landmark's IT division has been spinning off into a separate commercial venture with the concept of application oriented Information technology products and services to care to the requirements of the IT industry at large.

SOLUTIONS OFFERED:

AADHITIYA has in its portfolio the following solutions:

- Wireless Data Capture Solutions
- Biometric Based Solutions
- Security Solutions
- Retail Management Solutions for small, medium and large retail outlets
- Warehouse Management and Logistics
- B2B Collaborative services
- Financial Management Solutions
- Networking solutions both wired and wireless
- Internet, Intranet, Extranet and other Web Based Solutions.
- Hardware and Networking

The Vision:

To be the most vociferous proponents of application based information technology by designing, developing, implementing and providing products, solutions and services with business requirements as the basis of technology innovation.

The Mission:

Take every domain and provide need based information technology products, solutions and services using experts with hands on real world experience focusing on the future of the domain and delivering value addition to enhance its customer satisfaction.

1.2 . PROJECT OVERVIEW

A (computer) virus is a program (a block of executable code) which attaches itself to, overwrites or otherwise replaces another program in order to reproduce itself without the knowledge of the PC user. Most viruses are comparatively harmless, and may be present for years with no noticeable effect: some, however, may cause random damage to data files (sometimes insidiously, over a long period) or attempt to destroy files and disks. Others cause unintended damage. Even benign viruses (apparently non-destructive viruses) cause significant damage by occupying disk space and/or main memory, by using up CPU processing time, and by the time and expense wasted in detecting and removing them.

This project connotes to an anti virus program which is capable of removing the Bagle Worm & Mydoomnovarg type of virus. This project checks for the virus signature if it matches that will be removed.

Bagel Worm

Bagle is a mass-mailing worm that was found on 18th of January, 2004. The worm sends messages with the subject 'Hi' and random EXE attachment names. The worm installs a backdoor to infected machines. Bagle has been programmed to stop spreading on 28th of January.

Normally, Bagle variants search local hard drives of infected machines to harvest e-mail addresses, but Hyponnen said the new variants connect to a Web back-end server capable of generating unique e-mail addresses.

Bagel contains a backdoor that listens on a TCP port 6777 which is hardcoded in the worm's body. This backdoor component provides remote access to the infected computer. It can be used to download and execute arbitrary programs from the Internet.

When the worm is started it connects to a list of predefined web servers and tries to access a PHP file with certain parameters. One of the parameters is the TCP port where the backdoor is listening which suggests that this functionality is used to collect the addresses of infected computers.

"Bagle may have fooled us into initially thinking that it was all about getting attention, but it quickly became apparent that this was professional software, where the author was adding and disabling different functions," said Gordon. "It's really the first time a virus writer was paying attention to the details, and essentially following the CMMI process." This worm runs on Windows 95, 98, ME, NT, 2000 and XP.

MydoomNovarg

A new virus which can be spread by ZIP. email attachments has been reported. These may get through our email virus ...

W32.MyDoom is a rapidly spreading mass-mailing worm that uses its own SMTP engine to email itself to addresses harvested from infected systems, and installs a backdoor on infected systems on TCP port 1034. View this web cast to learn new information about this threat, as well as mitigating strategies and security solutions to prevent this worm from infecting your systems and to improve the overall security posture.

This worm sends email to addresses gathered from files with certain extensions, adding itself as an attachment. It uses Simple Mail Transfer Protocol (SMTP) to send out email with the following details:

Modules :

Virus scanning mode:

The scanning mode for the baggle worm as well as the mydoom virus can be done in two modes automatic and manual. A proper scanning goes with the root directory and respective action will be taken. Where as in manual operation, the directory will be searched for the identification of virus.

Automatic mode:

In this mode, our application will search for the baggle worm and all infected files in the root directory of the system as well as the registry values. And the infections got disinfected by means of removal of files and the registry values. The application will detect the infected files by checking the signature of the worm.

Manual mode:

In this mode, the user will be selecting the root directory or the different drives in which the worms got affected. The application will show the infections of worms as soon as the user selects the path. The user may have the option of taking appropriate action on the worms detected.

For the manual mode delete the registry value, terminate the running 'bbeagle.exe', Delete the worm from the Windows System Directory.

Beagle report and Mydoom report:

This part includes in both the manual and automatic mode, where the worms affected details, detection, removal and registry values will be collected before and after the action taken by the application. The different entities of the process will be given to the user. The registry values will be collected from this [HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ ] value.

Registry entries:

The baggle and mydoom virus might entered into the registry and had changed the values in the registry. After the removal of the worms in the system, still the registry entries exists. So the registry entries will be found by means of the signature of the types of worms. The different registry entities are D3DUPDATE, UID, FRUN.

Description of modules:

Virus scanning project consist of 2 modules. Each module have their own action and performance. The two modules are namely called as two mode they are

- ✓ Automatic mode
- ✓ Manual mode

Automatic mode

In this mode, our application will search for the baggle worm and all infected files in the root directory of the system as well as the registry values. And the infections got disinfected by means of removal of files and the registry values. The application will detect the infected files by checking the signature of the worm.

Operations

In this mode it will automatically checks for the bagel worm and mydoomnoarg virus .it will checks the all the registry entries with is stored in the system registry for checking the registry values we should know the registry value for each and every software which is install they are checked and the each and every root directory and files in the directory were checked automatically.

Manual mode

In this mode, the user will be selecting the root directory or the different drives in which the worms got affected. The application will show the infections of worms as soon as the user selects the path. The user may have the option of taking appropriate action on the worms detected.

For the manual mode delete the registry value, terminate the running 'bbeagle.exe', Delete the worm from the Windows System Directory.

Operations

In this manual mode also check for both bagel worm and mydoomnoarg virus. In this mode user should give the input (eg) which directory or file or registry values they have to specify at the run time .It help us to find and kill the virus and worm very quickly.

Existing system

we all know that for virus scanning there is lot of tools available. There is lot n lot company in al over the world the are not giving importants for the particular virus because developing cost of that particular tool was very high.for that only they the expense of the tool estimated and then start to develop.

Advantage of Existing sysytem

- ✓ We no need spend time with that tool when the scanning process starts
- ✓ The all tool have their own standards
- ✓ The software ie tool develop by that will undergo some tet likely alpha test beta test,function test ,integration test etc.
- ✓ It will scan the system for all kind of virus and worms

Disadvantage of Existing system

- ✓ Tools are developed by some organization ,the main aim of that company is to earn money through this tool, so cost of the project is very high .it cannot be used by all knid of people.
- ✓ Its very very difficult study the tool
- ✓ Some company may release only the exe of that particular software . if any damage if its cause the entire tool is waste ,it cause loss of money to the organization who is going to buy the particular damaged tool
- ✓ Scanning process will take more time, because it will scan entrie system for all virus minimally it will scan 100 to 150 signature of viruse and worms
- ✓ It will take more time

Proposed system

In my project it over comes some of the drawbacks which are not satisfied the programmer as well as the user who is going to use our tool. There is no tool that which is not completely destroy the or kill the virus which infect the entire system ie, our operating system. In ancient day it does not kill the virus fully.when ever operating system loaded the virus will be scan and delete that time. In our proposed system suppose a virus found it will scan in two way either automatic mode nor manual mode . suppose a virus found it will killed and the special signature is stored in a memory .once operating system loaded it checks for the particular signature found it will destroy the signature and stored to temporary memory.it will remain there until system is shutdown.

Advantage of proposed system

- ✓ In our organization we need to find bagel worm and mydoomnoarg virus so it will reduce the time
- ✓ Third party tool is much costlier then the tool which I have developed
- ✓ We can access the system which is connected in LAN, WAN .MAN we can access through the shared data .
- ✓ It will reduce the manpower
- ✓ We no need to check for all the signature in exceptional cases
- ✓ ts very easy to under stand the system

Disadvantage of proposed system

- ✓ This tool will not supportive to all the field .becaues only bagle worm and mydoomnoarg virus .
- ✓ It mainly helps the people who take care about the process of sending and receiving the email .This virus and worm cause damage .
- ✓ Mostly banking and financial people use thie project It maintain the record accuretly and legibly .
- ✓ It does not support lower version of windows.

SCOPE AND OBJECTIVE OF THE PROPOSED SYSTEM

Antivirus system is model to protect our system from infections caused by the worms and viruses.This system provide some features to find worm which are affecting the entire system directory and registry values.

Scope of the product within the PCs. Scanning and detecting virus have the following modules.

VIRUS SCANNING MODE

Virus are scanned from the registry by running the created Exe file .It scans the virus by two mode

1. Automatic mode
2. Manual mode

AUTOMATIC MODE

It scans the root of the directory and the registry if the virus or worm found it will detect and remove.

MANUAL MODE

User may select the path for scanning either directory or the Root driver.

GENERAL DESCRIPTION

Virus

A computer virus is a program –a piece of executable code that uniqe ability to replicate.t consume storage space and memory and degrade overall performance .

worm

A computer worm is a self –contained program . Set of program that able to spread function copies to itself or segmented to other computer system.

References

The system refers the user with very user friendly screens for their convenience. The approach is done in such a manner that it

rview

This document helps the software developer to design and develop tware with a standard approach where all the necessary constraint is vided as per the requirement fulfills all the requirements of the organization.

er characteristic

User friendly software with essential requirement. Not onlythe program eveloper all kind of people may use because easy for work.

Specific requirements

Introduction

This part deal with the necessary requirements for the software to make all the function highly performable

List of Inputs

Automatic mode

Pressing appropriate button it automatically refer the for the particular Virus or worm and then it check with the directory as well as the registry value.

Manual mode

In manual mode user have to specify the directory Which is going to be checked or scanned by clicking or giving appropriate signature for that particular virus

Information processing required

1. It compare the registry value and the data persent in Root directory.
2. It check each and every root directory and driver and registry values line by line.
3. If virus is found then they indicate that the virus found.
4. Remove the virus by automatically or manually.

List of outputs

1.**D3DUPDATE**, UID, FRUN the registry entities found

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Run
d3dupdate.exe = "%System%\bbeagle.exe"
```

UID

```
HKEY_USERS\%SystemInfo%\Software\Windows98
Uid = <Numeric Value>
```

FRUN

```
HKEY_USERS\%SystemInfo%\Software\Windows98
Frun = %SystemInfo%
```

EXTERNAL INTREFACE REQUIRED

User should have good communication for reading and understanding the process which is carried each and every action.

Hardware interfaces like modem, telephone connection, internet connection and processor should be atleast Pentium III or higher , 128 RAM or higher . Software interface like Microsoft Dot Net Frame Work 1.1, operating system windows 98 or higher .

CHAPTER 2

2.3. SYSTEM REQUIREMENTS SPECIFICATION

HARDWARE SPECIFICATION

PROCESSOR	: Intel Pentium IV Processor
SPEED	: 1.7 GHZ
RAM	: 128MB
HARD DISK	: 20 GB (MIN)
NETWORK ENVIRONMENT	: LAN or WAN with Windows 2000 Server or Windows XP
INTERNET FACILITIES	: Internet should be provided for Server access
MOUSE	: 2 or 3 button mouse
KEYBOARD	: 101 key Keyboard.

SOFTWARE REQUIREMENT

DEVELOPMENT PLATFORM	: Windows 2000 or Windows XP
FRONT-END	: Microsoft .NET(VB.NET)

2.3 SOFTWARE OVERVIEW

Introduction to the .NET Framework

The .NET Framework is a managed type-safe environment for application development and execution. The .NET Framework manages all aspects of your program's execution. It allocates memory for the storage of data and instructions, grants or denies the appropriate permissions to your application, initiates and manages application execution, and manages the reallocation of memory from resources that are no longer needed. The .NET Framework consists of two main components: the common language runtime and the .NET Framework class library.

The common language runtime can be thought of as the environment that manages code execution. It provides core services, such as code compilation, memory allocation, thread management, and garbage collection. Through the common type system (CTS), it enforces strict type-safety and ensures that code is executed in a safe environment by also enforcing code access security.

The .NET Framework class library provides a collection of useful and reusable types that are designed to integrate with the common language runtime. The types provided by the .NET Framework are object-oriented and fully extensible, and they allow you to seamlessly integrate your applications with the .NET Framework.

Languages and the .NET Framework

The .NET Framework is designed for cross-language compatibility, which means, simply, that .NET components can interact with each other no matter what supported language they were written in originally. So, an application written in Microsoft Visual Basic.NET might reference a dynamic-link library

(DLL) file written in Microsoft Visual C#, which in turn might access a resource written in managed Microsoft Visual C++ or any other .NET language. This language interoperability extends to full object-oriented inheritance. A Visual Basic.NET class might be derived from a C# class, for example, or vice versa.

The Structure of a .NET Application

To understand how the common language runtime manages code execution, you must examine the structure of a .NET application. The primary unit of a .NET application is the assembly. An assembly is a self-describing collection of code, resources, and metadata. The assembly manifest contains information about what is contained within the assembly. The assembly manifest provides:

- ✓ Identity information, such as the assembly's name and version number
- ✓ A list of all types exposed by the assembly
- ✓ A list of other assemblies required by the assembly
- ✓ A list of code access security instructions, including permissions required by the assembly and permissions to be denied the assembly

Compilation and Execution of a .NET Application

When you compile a .NET application, it is not compiled to binary machine code; rather, it is converted to IL. This is the form that your deployed application takes-one or more assemblies consisting of executable flies and DLL files in IL form. At least one of these assemblies will contain an executable flies that has been designated as the entry point for the application.

- ✓ The .NET Base Class Library
- ✓ The Connection Object
- ✓ The DataReader Object
- ✓ The DataAdapter Object

Advantages of .Net Framework

- ✓ Consistent programming model
- ✓ Multi-platform Applications
- ✓ Multi-language integration
- ✓ Automatic resource management
- ✓ Ease of deployment

Features of Visual Basic .NET

- ✓ Inheritance
- ✓ Constructors & Destructors
- ✓ Overloading
- ✓ Overriding
- ✓ Structured exception handling
- ✓ Multi threading

CHAPTER 3

SYSTEM ANALYSIS

INTRODUCTION

System analysis is concerned with investigating and analyzing which is used to gain an understanding of the existing system and what is required. It is a general form refers to orderly structured process for identifying and problem solving.

System analysis is the application of the systems approach to problem solving using computers. The ingredients are systems elements, processes, and technology. This means that to do systems work, one needs to understand the systems concept and how organizations operate as a system.

System analysis is a process related to four significant phases namely study phase, design phase, development phase and operation phase. The definition of the system analysis is not only the process of analysis but also that of synthesis. System analysis is actually a customized approach to the use of the computer for solving problem.

Many existing technologies allow clients to share files amongst themselves. The main improvement this system offers over the other available a technology is that the files will be shared securely. The security aspects will involve encryption of the file before it is sent and subsequent decryption by the recipient of the file. This means only the intended recipient will be able to read the contents of the file, so if the data transmission were intercepted by a third Party, it would be undecipherable.

Another security measure of the system should allow it to detect invalid users. Therefore, if a hacker were able to break into a communication stream, the system would be able to validate the authenticity of the user and then take appropriate action.

CHAPTER 4

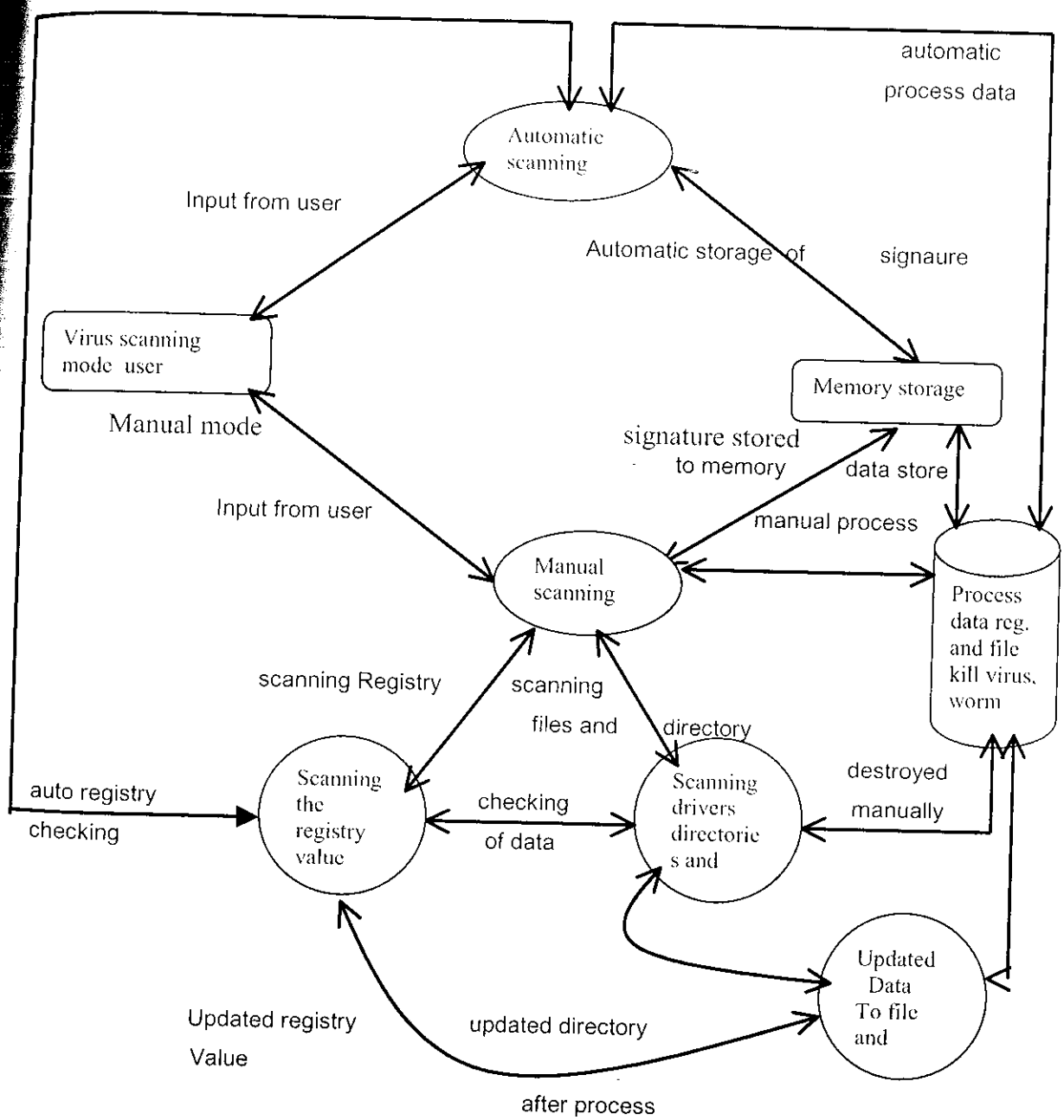
SYSTEM DESIGN

INTRODUCTION

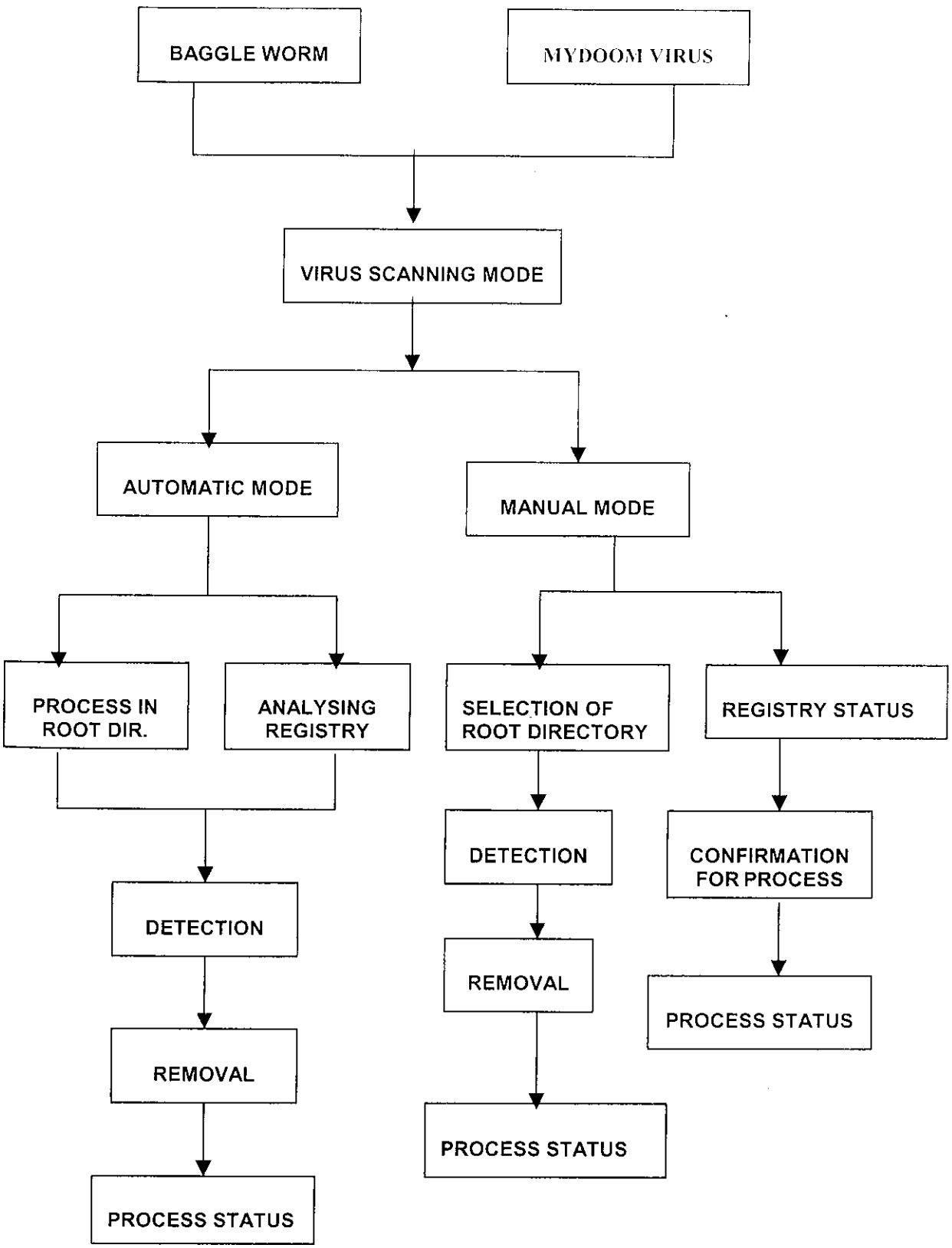
The original thinking behind this system was it could be deployed in a commercial environment, where a group of users who require the need to share files amongst themselves in a secure manner could subscribe to the service, and guarantee their authenticity. Therefore, if it were to be deployed in a business environment, only authorized users would be able to gain access share files with each other.

File sharing can already be achieved with a standard network operating system, as access permissions can be set to directories, giving access only to authorized users. However, this is not the safest or most efficient method of sharing files as passwords can be obtained and transmitting files over a wide area using a network can be slow.

4.1.Data flow diagram



4.2.PROCES DIAGRAM



CHAPTER-5

IMPLEMENTATION

5.1 SYSTEM TESTING

Software configuration includes a software requirements specification, a design specification and source code. Test configuration includes a test plan and procedure any testing tools and test cases and their expected.

User requirements test

This is the test done at the time of requirements document URS(User Requirement Specification). In this, the requirements are tested for clarity, redundancy, feasibility and objectivity. As soon as the requirements are tested, the URS can be helpful in preparing the acceptance test plan so that the user tests the software according to the URS.

System requirement test

From the URS we produce SRD(System Requirement Document) which tests the validity of the system at the client end. As soon as the document is ready, they can make a plan for the systems test conducted by the development organization before coordinating the acceptance test.

Effective testing early in the process translates directly into long-term cost saving from a reduced number of errors. The first trust for system is to see whether it produces correct outputs. The test data may be artificial or live.

The software, which has been developed, has to be tested to prove its validity. Testing is considered to be the least creative phase of the whole cycle

of system design. In the real its is the phase, which helps to bring out the creativity of the other phases makes it shine. The "Port Trust Estate Management System (FHMC, CISF, LAND) using the following techniques of software testing.

1.White Box Testing

By using this technique it was tested that all the individual logical paths were executed at least once, all the logical decision were tested on both there true and false sides. All the loops were tested with data in between the ranges and especially at the boundary values.

2.Black Box Testing

By using this technique, the missing functions were identified and placed in their positions. The errors in the interfaces were identified and corrected. This technique was also used to identify the initialization and termination errors and correct them.

Software Testing Strategies

Any software has to be tested with pre-planned strategies. As Roger Pressmen states, the preparation for testing should start as soon as the design of system starts, to carry out the testing in an efficient manner certain amount of strategic planning has to be done. Any testing strategy must incorporate test planning, test case design, test execution and the resultant data collection and evaluation.

6.1 Unit Testing

In the lines of this strategy all, the individual functions and modules were put to the test independently. By following this strategy all, the errors in coding were identified and corrupted. This method was applied in combination with the white and black box testing techniques to find the errors in each module.

6.2 Integration Testing

Again this software testing strategy has different approach in which integration is carried out from the top level module to the bottom and the bottom up approach in which integration is carried out from the low level module to the top.

The modules are tested using the bottom up approach by introducing stumps for the top-level functions.

This test used to identify the errors in the interfaces, the errors in passing the parameters between the functions and corrects them.

Validation Testing

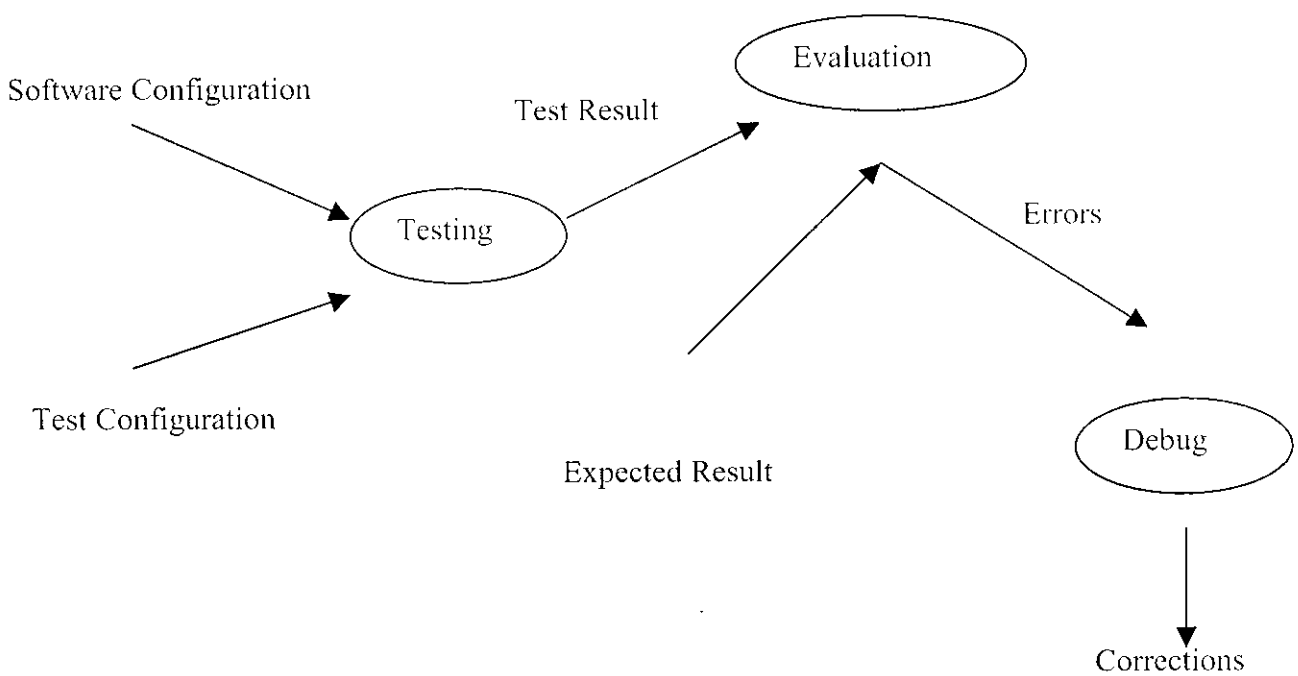
Validation testing is done to validate the inputs given by the user. The user inputs are checked for their correctness and range. If there are errors, the error message is given and the user is prompted again to enter the new value. If the user types some characters in the Number field an error message and it is demonstrated in the following figure.

6.3 System Testing

Software testing is an important element of software quality assurance and represents the ultimate review of specification, design and coding. There are rules that can serve as testing objectives. They are

- Testing is a process of executing a program with the intent of finding an error.
- A good test case is one that has high probability of finding an undiscovered error.
- A successful test is one that uncovers an undiscovered error.

Testing Information Flow



Acceptance Testing

Acceptance testing is sometimes performed with realistic data of the client to demonstrate that the software is working satisfactorily. It includes database features like integrity, consistency, security and validity.

The project is tested with different types of data to verify the quality of the program. Some validation procedures used to verify are,

- To verify whether the data specified is a valid one.
- To verify whether any inputs left unfilled.
- To verify whether the amount specified is a valid amount.
- Reports are not generated when the database contains null data.
- Message box is prompted to verify whenever an updating is done.

After testing the system and find it successful to put the new system into operation, there are different techniques that can be used to replace an existing system with the new system.

Direct Change over

In this technique, the existing system is replaced by the proposed system after ensuring that system objectives are met. This method is adopted in this project. This software is successfully demonstrated to Chennai Port Trust.

Parallel run

The proposed system is put into operation in parallel with the existing system for a period of 60 days to monitor the performance. The existing system becomes inspirational if the proposed system produces the expected results.

Pilot run

In pilot run, the system is tested with available result of the existing system. The performance of the system is studied with the latest data.

Staged Change over

In this technique the existing system becomes inspirational if all the stages are successfully implemented. The whole project is through the main menu. Through the main menu all the modules and reports are linked and called from this menu as and when required by selecting the respective bars in the main menu. When any changes or updating is made, reports are automatically updated.

5.2 MAINTENANCE

The process of making changes and modifications to the system after it has been delivered implemented and is in use called software maintenance.

Corrective Maintenance

It is concerned with fixing reported errors in software. They are coding errors and design errors.

Adaptive Maintenance

It is concerned with changing the software to source and to adapt to the new and changing environment.

Defective Maintenance

It involves implementing new functioned or non-functional system requirements to ensure more effective execution of the system.

Perceptive Maintenance

It mainly deals with accommodating new or changed users requirements. It also includes activities to increase the system performance or to enhance its user interface. The objective of perceptive maintenance should be to prevent failures and optimize the software.

Preventive Maintenance

It concerns activities aimed at increasing the system's maintainability such as updating documentation adding comments, improving modular structure of the system.

CHAPTER 6

CONCLUSION

With the help of our antivirus software we will protect our software and operating system of our personal computer .it will find the virus and kill the virus. It is checked and verified by **aadithya infomedia Chennai.**

We conclude that our software is uvery useful for all the software developers and the programs who's going to develop the software's.

It is mainly focused on bagel worm and mydoomnoavg virus if find and kill it both automatically and manually.

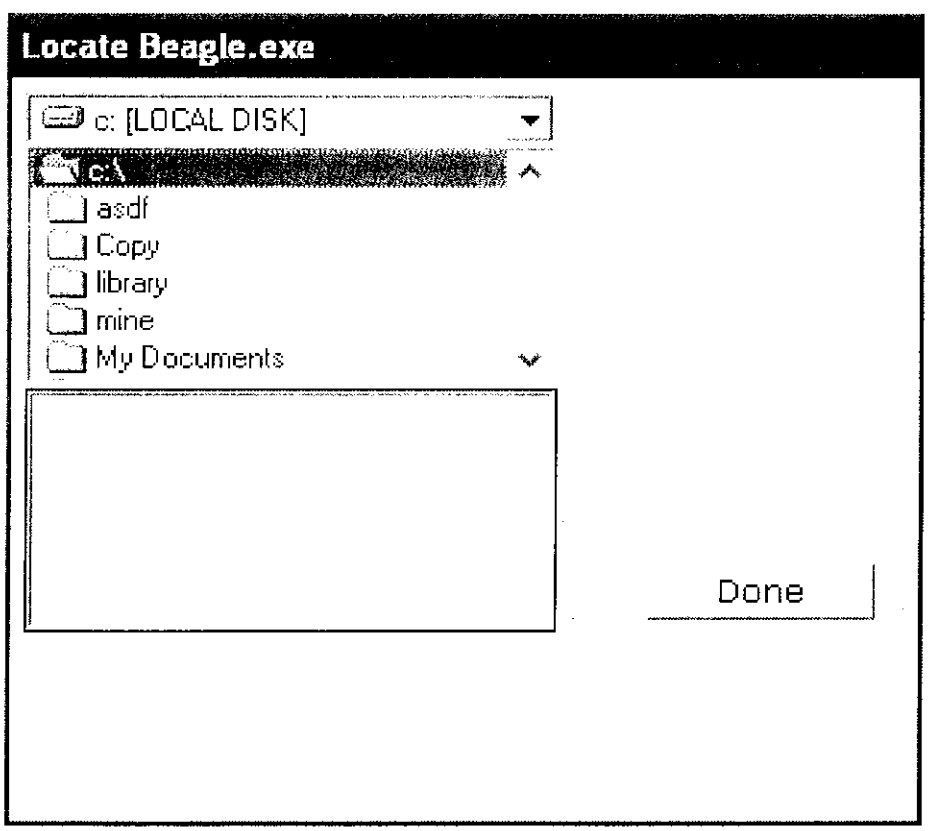
This is the tool which helps the programmer to find what type of virus and worm affect the system. Mostly banking and financial people use this project It maintain the record accuretly and legibly.

APPENDICES – SCREEN LAYOUT

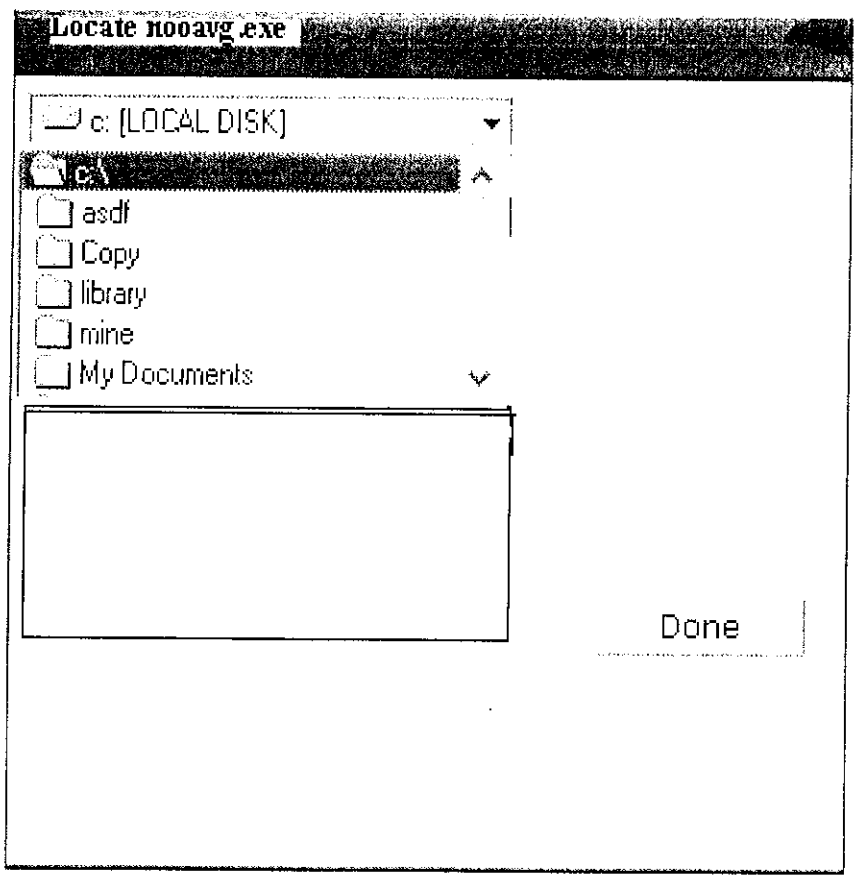
INPUT FOR VIRUS SCAN

INPUT:

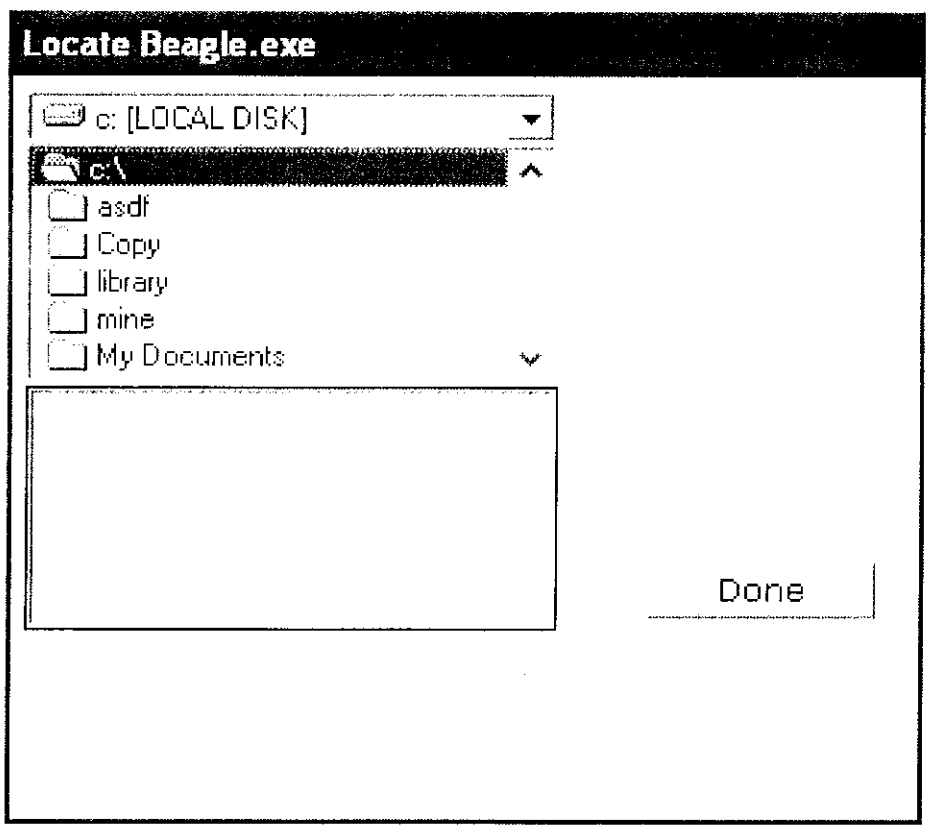
AUTOMATIC MODE FOR BAGEL WORM



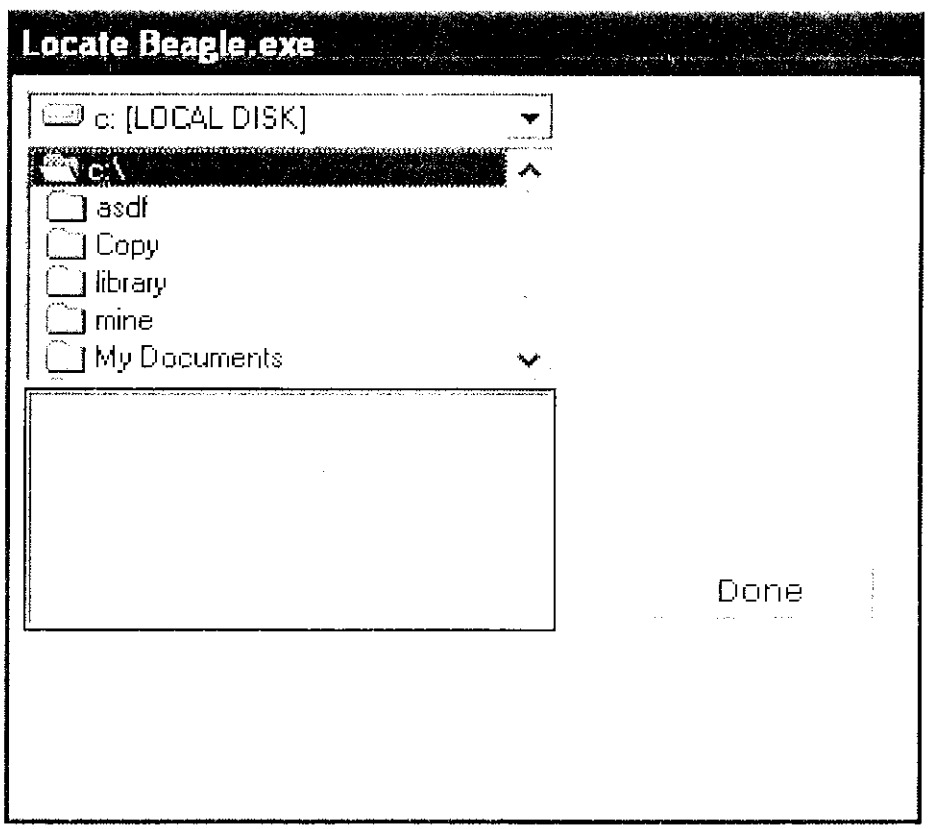
AUTOMATIC MODE FOR NOARG VIRUS



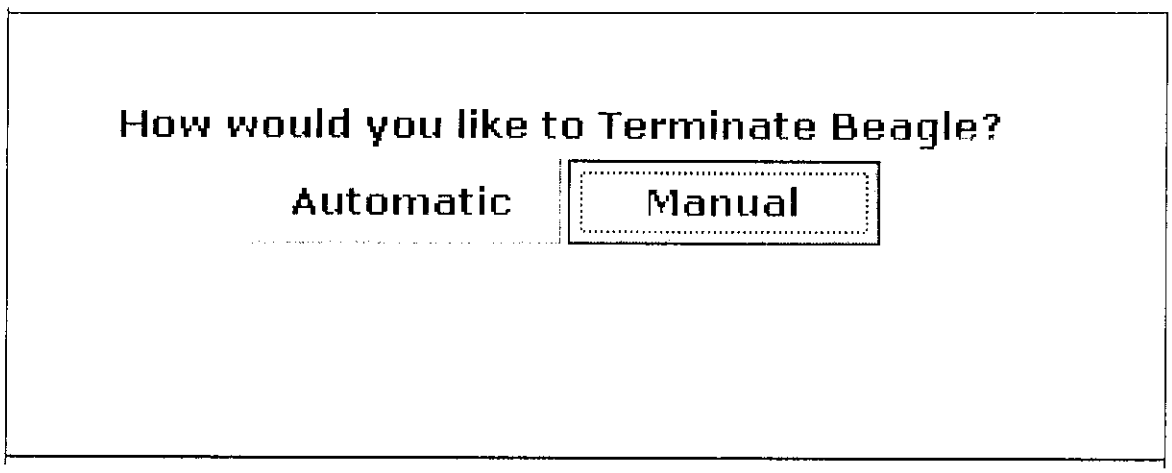
OUTPUT
AUTOMATIC MODE FOR BAGEL WORM



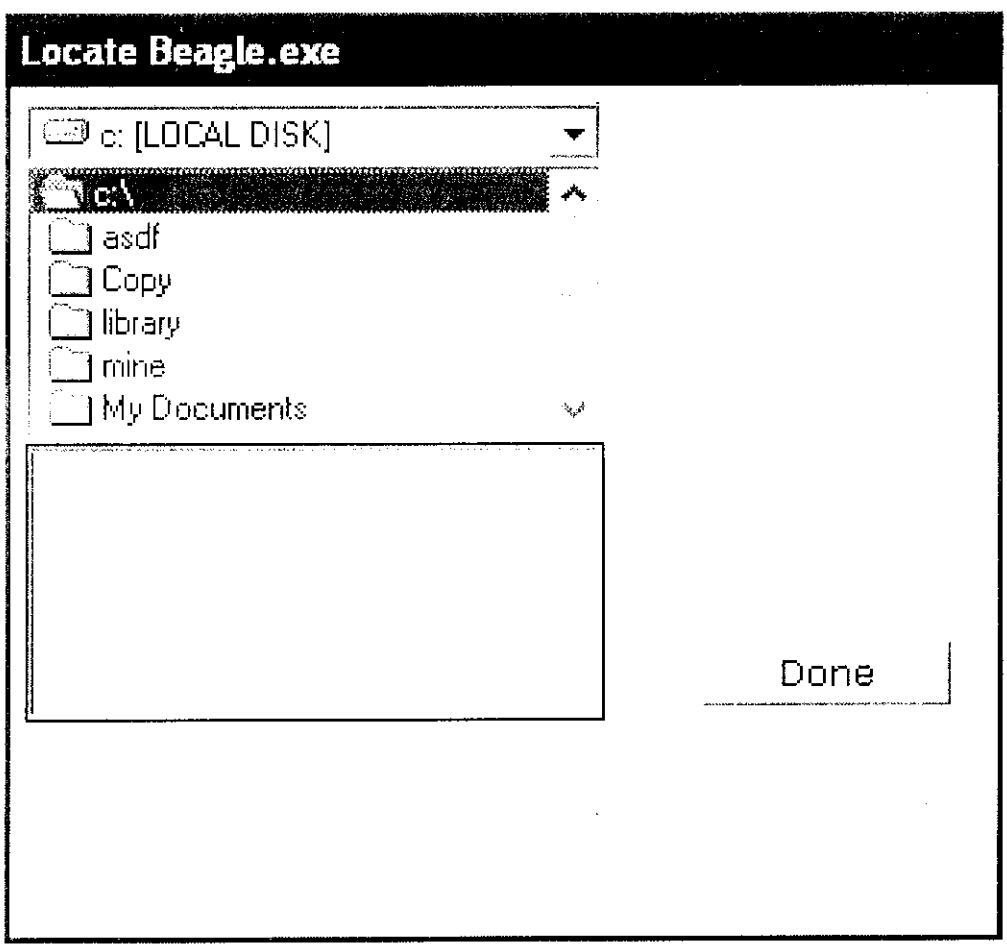
AUTOMATIC MODE FOR NOARG VIRUS



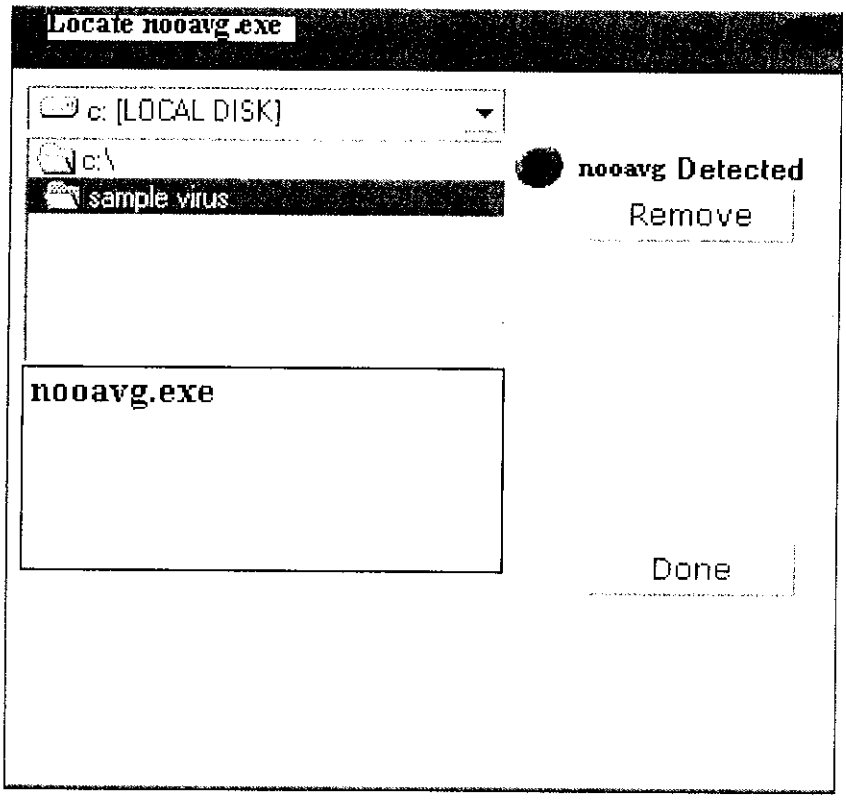
INPUT FOR MANUAL MODE



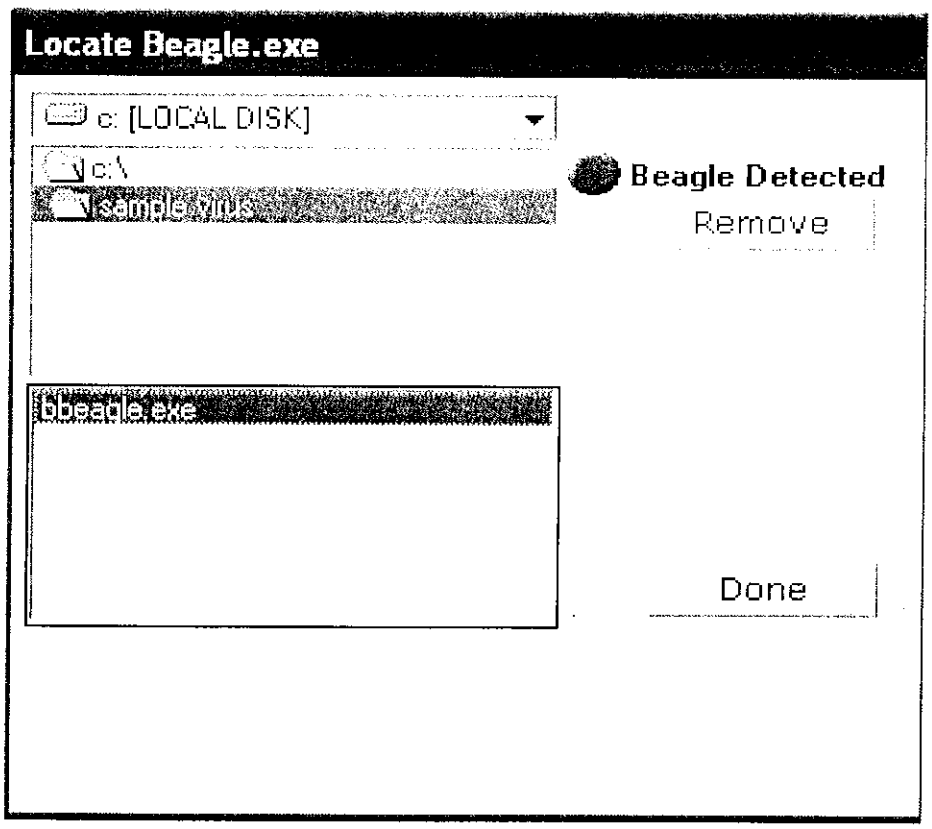
MANUAL INPUT FOR BAGEL WORM



OUTPUT OF MANUAL MODE



OUTPUT FOR MANUAL MODE



Sample coding for bagel worm

```
<?xml version="1.0" encoding="utf-8"?>
<UpgradeLog>
   <Settings>
      <Setting
         Name = "LogFile"
         Value = "BeagleHunter.log"  />
      <Setting
         Name = "GenerateInterfacesForClasses"
         Value = "FALSE"     />
     <Setting
         Name = "ProjectName"
         Value = "BeagleHunter"  />
     <Setting
          Name = "OutputName"
         Value = "BeagleHunter.vbproj"   />
    <Setting
         Name = "OutputDir"
         Value = "I:\BeagleHunter\BeagleHunter.NET"   />
    <Setting
         Name = "ProjectPath"
         Value = "I:\BeagleHunter\BeagleHunter.vbp"   />
   <Setting
         Name = "MigrateProjectTo"
         Value = "0"
     </Settings>
   <File
      OldPath = "I:\BeagleHunter\fMain.frm"
      NewPath = "I:\BeagleHunter\BeagleHunter.NET\fMain.vb"
```

Sample coding for mydoomnoarg

```
<?xml version="1.0" encoding="utf-8"?>
<UpgradeLog>
  <Settings>
    <Setting
      Name = "LogFile"
      Value = "NovargHunter.log"/>
    <Setting
      Name = "GenerateInterfacesForClasses"
      Value = "FALSE"/>
    <Setting
      Name = "ProjectName"
      Value = "NovargHunter" />
    <Setting
      Name = "OutputName"
      Value = "NovargHunter.vbproj" />
    <Setting
      Name = "OutputDir"
      Value = "I:\Novarg_Hunter\NovargHunter.NET" />
    <Setting
      Name = "ProjectPath"
      Value = "I:\Novarg_Hunter\NovargHunter.vbp" />
    <Setting
      Name = "MigrateProjectTo"
      Value = "0"/>
  </Settings>
  <File
    OldPath = "I:\Novarg_Hunter\RegisterEX.cls"
    NewPath = "I:\Novarg_Hunter\NovargHunter.NET\RegisterEX.vb"
```

BIBLIOGRAPHY

Books

1. The complete references for vb.Net- V. Sourcesafe .
2. Special Edition Using vb.Net by Bulletin v3.0.1. ,Jelsoft Enterprises Ltd.

Web Sites

1. www.palisade.com
2. www.owlnext.sourceforge.net
3. www.altavista.com