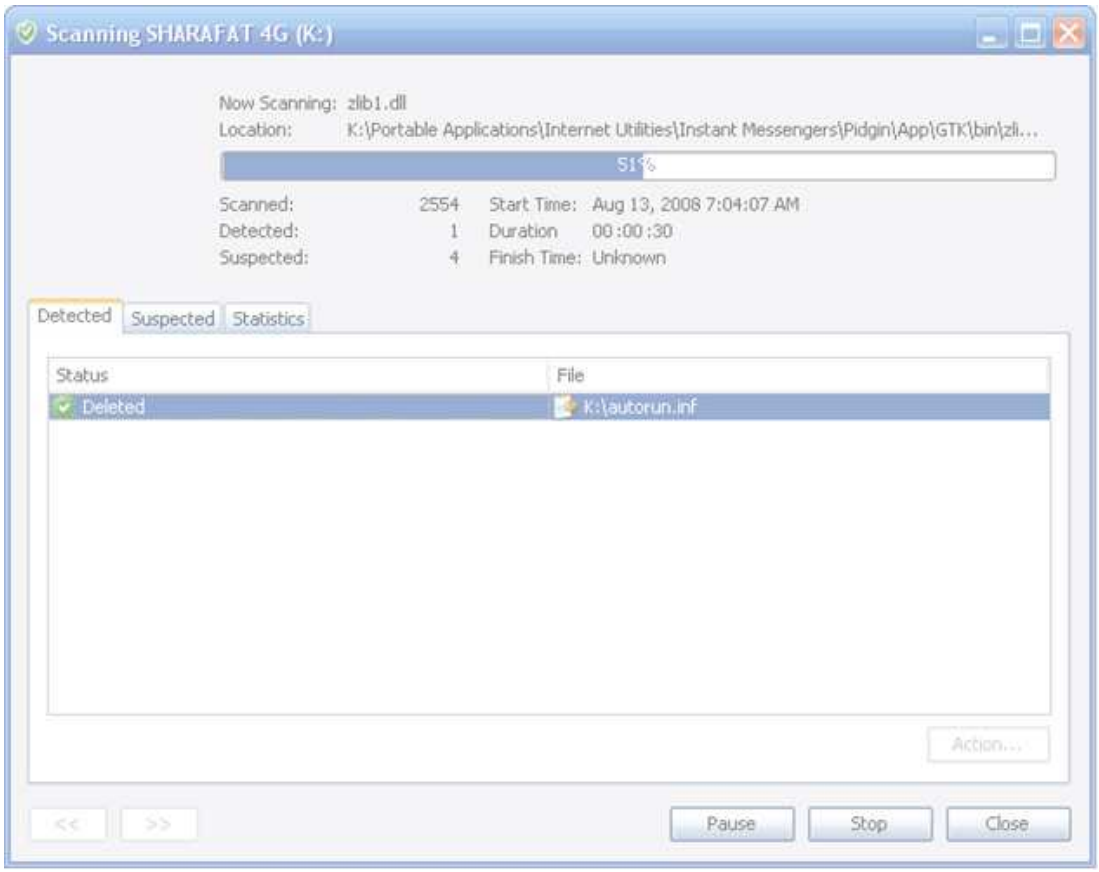
SOFTWARE PROJECT

Developing an Antiworm Solution

[USB WORM PROTECTION]



Submitted By:

Sharafat Ibn Mollah Mosharraf

Roll No. 01

12th Batch,

Dept. of Computer Science & Engineering,

University of Dhaka

TABLE OF CONTENTS

OBJECTIVE

The goal of this project is to develop a software which would scan USB mass storage devices as well as local hard disk drives for worms.

OVERVIEW OF THE SOFTWARE

The software has the following major functionalities:

- Scanning a USB mass storage device whenever it is plugged in.
- Scanning multiple devices simultaneously.
- Displaying detected and suspected worm files and prompting the user for action.

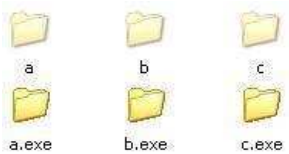
CORE LOGIC – WORM DETECTION

Unlike traditional antimalware softwares, this software doesn't use any type of dictionary-based worm detection. Worms carry out some regular tasks in a similar manner. The software detects worms according to these manners. Following are the tasks which a worm does whenever a removable mass storage device is connected to the system:

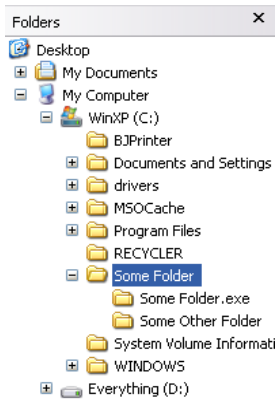
- At the root level of a drive, a copy of the worm executable file is placed as a hidden file.

- An autorun.inf file is placed there so that whenever a user double-clicks on the drive icon, the worm file is executed.
- A copy of the worm file renamed as "New Folder.exe" with an icon of a folder is placed there.
- The Brontok worm places its own copy at the root level renaming it to "Data" followed by the current user-account name.

- In some cases, the folders at the root level are made hidden and copies of the worm file renamed to those folder names along with icons of folders are placed there.



- Inside each folder in a drive, a copy of the worm file with the same name as the folder along with the icon of a folder is placed.

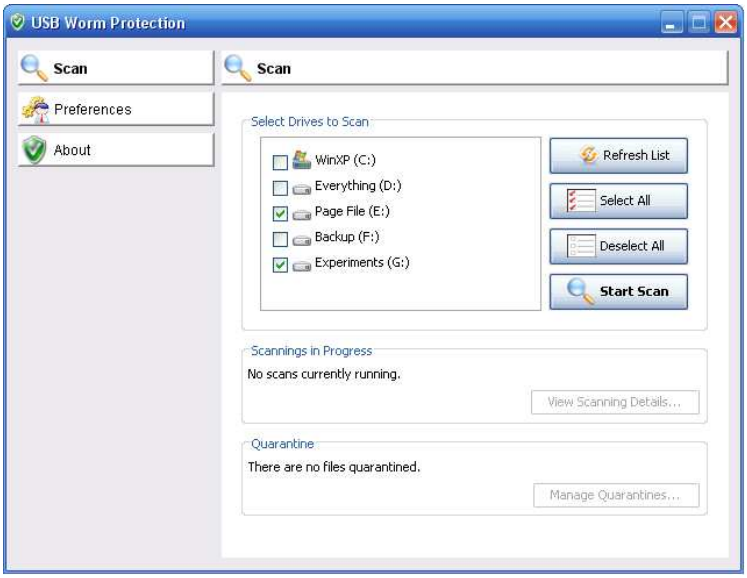


FEATURES

1. **The main window and the scan panel**

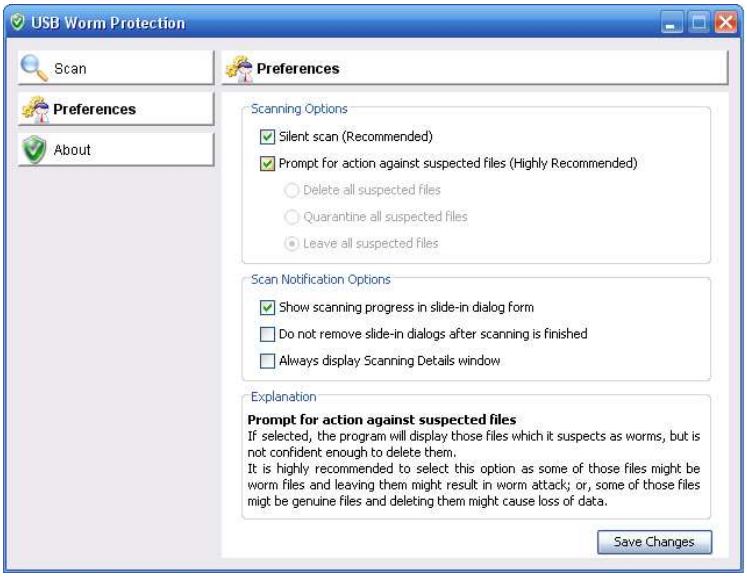
   From the main window, various tasks such as scanning devices, setting preferences etc. can be performed.

   From the scan panel, drives can be selected for scanning. Scanning details as well as quarantine information can also be accessed from this panel.



2. **The preferences panel**

   From this panel, various preference options can be set. Whenever the mouse is hovered over an option, the explanation of that option is presented at the bottom of the panel.

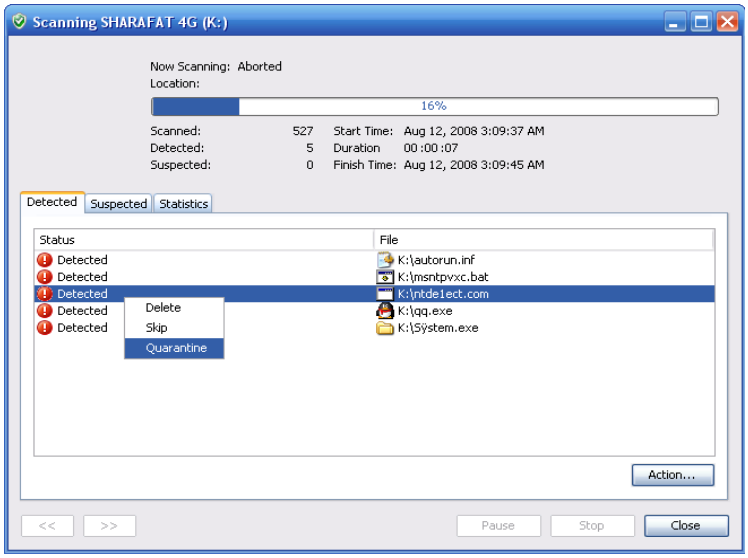


3. The about panel

Information about the software and its writer is presented here.

4. The scanning details window

Details scanning information is presented in this window. User is given the choice of taking any action against any file detected or suspected.

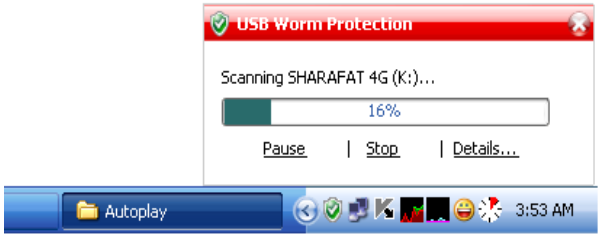


5. The pause protection dialog

From this dialog, on-access protection can be paused from several minutes up to several hours, until the program restarts, or until the user explicitly enables the protection.

6. The slide-in message

Whenever a USB mass storage device is plugged into the system, a slide-in message appears from the bottom-right corner of the screen indicating its scanning progresss.



CUSTOM CLASSES USED

Main	Here all the objects (such as the main window, scan frame, program tray icon etc.) are initialized.
MainWindow	Class for the main window.
ProgramTrayIcon	Class for the program tray icon.
ScanPanel	Class for the drive scanning panel.
About	Class for the about panel.
PreferencesPanel	Class for the preferences panel.
ScanFrame	The scanning details window.
Scan	Here all the file scanning is performed.
ScansManager	Simultaneous scans are managed though this.
Preferences	For setting user preferences.
PauseProtection	For disabling on-access protection.
SlideInScanPanel	The slide-in message window indicating scan progress of plugged-in USB mass storage devices.
SlideInDialog	For displaying other slide-in notification dialogs.
SlideInNotification	For animating the slide-in messages.

LIMITATION

This software can only prevent worms from affecting the system. If the system is already affected by worms, it will not be of any use.

FUTURE PLANS

- Adding the capability of curing a worm-affected system.
- Providing user with more information about detected worms.
- Enhancing the GUI.