Fifth Generation Systems

Search & Destroy Help Contents

Introduction
What is Search & Destroy?

Search & Destroy is a Windows compatible Specific Virus scanner written by BRM Technologies and Licensed exclusively to Fifth Generation Systems . It is designed to perform quick scanning of files on Network drives, Fixed Disks, and Floppy Drives as either a foreground or a background operation within Microsoft Windows version 3.x. A DOS version of Search & Destroy is also included in order to scan for viruses from DOS.
A TSR is included which monitors the activity of the DOS operating system and conventional memory to provide immediate warning of an attempt by a virus to become resident and possibly infect program files. A Windows version of the TSR is also available, to monitor the Windows environment for known viruses which are launched or attempt to become resident within Windows. The TSR will also alert the user to any disk or diskette that is accessed from Windows or DOS.

For Information about viruses:

A Little About VIRUSES

A Little About VIRUSES

First Developed in 1983 by a student at the University of Southern California in 1983, Computer viruses have grown in numbers and variance in the last nine years. According to the NCSA, over 38,000 different "strains" will be in circulation by 1994. Though many are innocuous, having not been written with malevolent intent, all present a risk to both the integrity of your data and the efficiency of computer resources. Some, however specifically present a real and ever present danger, having been specifically designed to damage or corrupt data both at the system and application level.

What is a Virus?

A Virus is a program or segment of a program which is designed to replicate itself by the use of any program or segment of a program that is executed consistently during the normal operation of some computer system. Attaching itself to the beginning (or end) of such code and modifying the program to execute the virus, then itself, the virus will be loaded into memory at some point, thus allowing it to infect other programs or program segments. Hence, this type of computer program is called a virus.

With all viruses, any file infected will reflect the fact by a certain characteristic code or pattern, known as a signature. Once a new virus is detected and scrutinized, it is possible to detect them with a high degree of confidence by either monitoring the memory and operating system of a computer (TSR monitors), comparing the data on storage devices to known signatures (Scanners), or a combination of both. Even viruses designed specifically to defeat such defenses have been neutralized by modern virus scanners and TSR monitors. Unfortunately, with the proliferation of new viruses and variants, it is always a possibility that a new, as yet undiscovered virus will be invisible to an up to date virus scanner. For complete assurance and 100% protection, an automatic virus system such as **Untouchable** is necessary, which keeps track of the integrity of your file system by keeping a history of file vital-statistics. With a product such as Search & Destroy, you still have a high degree of security, since a new virus will most likely be encountered where there is a lot of software traffic. Exercising care and following a few tips can keep your computer system virus free.

Viruses Types
Symptoms

Virus Types

Most Viruses will become "active" by being loaded into resident memory in some way. Viruses which cause damage without becoming resident are referred to as either ***trojans*** or ***bombs***. These viruses have become relatively outdated in recent years.
Memory resident viruses work in different ways, and can be classified by their method of replication

EXE or COM (File) Infectors:

These viruses will become resident from the execution of an already infected EXE or COM program. After loaded in to memory by their "host", they will then monitor the activity of the operating system and infect any program which runs attaching a duplicate of itself to the program file stored on disk. Should that program file be transferred and executed on an uninfected machine, yet another file will become infected on that computer. If allowed to continue unhindered, the virus replicates geometrically, which can soon result in all the computers of a large organization becoming infected.

One variety of this type of virus is the stealth virus, which when resident, subtracts its signature from any file that is already infected that is loaded into memory, thus masking themselves from virus scanners.

Boot Infectors:

These viruses infect a disk or diskettes ***boot code***, which is executed when a system disk or diskette is used to ***boot*** a computer. The viruses replaces the boot code on disk, and relocates the original boot code to another location. When the system boots, the virus becomes resident before the operating system loads, either slowing system performance or waiting for a trigger event to perform some task, usually destructive. Each time this boot virus is run, it searches for other boot disks and diskettes to infect.

Partition Table Infectors:

A variety of Boot Infectors, replacing a fixed disk's ***partition table***, relocating the fixed disk's original partition table to another location. The virus then loads into memory before the hard disk information is loaded, searching for other fixed disks to infect. Once resident, these viruses also usually perform some task when activated by some event, usually destructive.

<u>Symptoms</u>

Symptoms

Though some viruses are undetectable, having no side effects, many viruses can cause strange or erratic behavior in the operation of a computer and its applications. Here is a brief listing of common danger signs.

Changes in program file size
Changes in program file date and time stamp
Slower program load times
Slower execution speed.
Uncommon error messages becoming more frequent
Unexplained reduction in available memory
Unexplained disk activity
Missing or corrupted data
Abnormal program termination

Using This Help System

This help system is a windows hypertext document that has the feature of allowing the user to quickly access referenced topics in other parts of the document. Whenever a topic is referenced like this: Click Here to Get Nowhere, you can point the mouse cursor at the phrase and click. The page which deals with that topic will then be displayed.

The Contents page can be used to jump to any section within the manual. All sections are listed here, organized by category.

An alphabetized Index is also available, for accessing certain sub-topics.

The keyboard commands used by SDSCAN follow the standard windows conventions. Wherever possible, the keyboard commands for the procedures and menu commands will be described. When keys are specified, they will be displayed in bold (ie **Spacebar**).

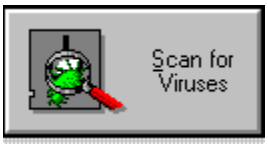
At times, key combinations will be specified to select commands. A keyboard command shown as

(**ALT-K**)

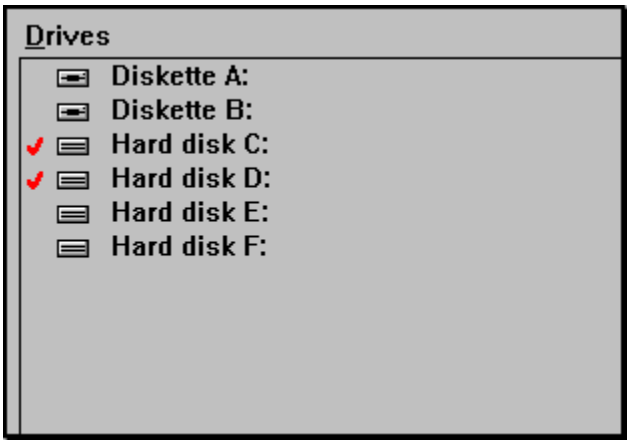
means to depress and hold the **ALT** key, and press the letter **K**.

Procedures

The SDSCAN Main Panel



After SDSCAN is opened, the main panel display will show a Drive selection box to the left which displays all local and network drives detected on your system. By default, all local hard drives will be selected with a check mark. Below the file selection box are three buttons which can be used to globally select all local hard drives, floppy drives, and network drives for scanning. A grayed out button will be displayed if no such drive type is detected.



Keyboard users can use the **TAB** key to switch between the buttons and the **Drive Selection Window**. The **Spacebar** can be used to select/deselect individual drives.

Three buttons are provided below the Drive Selection Window for selecting drives. Alt key combinations can be used to select them. Click on the buttons below for more information.

Selecting/Deselecting Drives to Scan
Scanning While Minimized

Scanning Hard Drives

To scan hard drives, click on the hard drives button. Keyboard users may select this button by typing <**ALT-A**>. All hard drives should have a red check mark displayed to the left. Then click on the **Scan for Viruses** button (Keyboard users: <**ALT-S**>).

Selecting/Deselecting Drives to Scan
The SDSCAN Main Panel

Scanning Floppy Drives

To scan a floppy drives, click on the **Floppy Drives** button. Keyboard users may select this button by typing <**ALT-F**>. The floppy drives will alternately be selected, first A:, then B:, etc. Verify that the selected diskette drive has a diskette inserted and the drive door is closed. Click on the **Scan for Viruses** button to begin the scan (Keyboard users: <**ALT-S**>).

Selecting/Deselecting Drives to Scan
The SDSCAN Main Panel

Scanning Network Drives

Search & Destroy can scan files which reside on **Novell Netware** volumes.

To Scan all Network drives (volumes), click on the **Network Drives** button. Keyboard users may select this button by typing <**ALT-N**>. All volumes displayed in the file box will be selected. Only Novell volumes will be selected. Click on the **Scan for Viruses** button to begin scanning.
(Keyboard users: <**ALT-S**>)

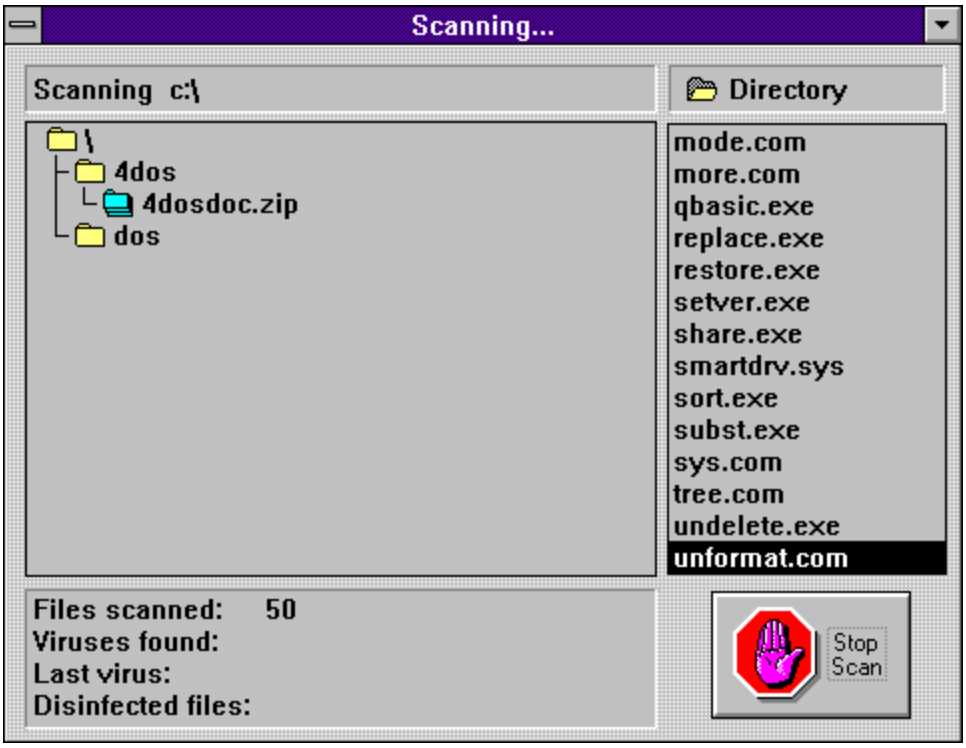
Selecting/Deselecting Drives to Scan
The SDSCAN Main Panel

Selecting/Deselecting Drives to Scan

Individual drives or combinations of drives can be selected or deselected for scanning to suit your current needs. Point to the desired drive in the Drive Selection Box and click once. Keyboard users may use the Tab key to select the Drive Selection Box and use the arrow keys to outline the desired drive or network volume. Press the **Spacebar** once. The outlined drive will be selected.
Click on the **Scan for Viruses** button or <**ALT-S**> to begin scanning Drives may be deselected in the same manner.

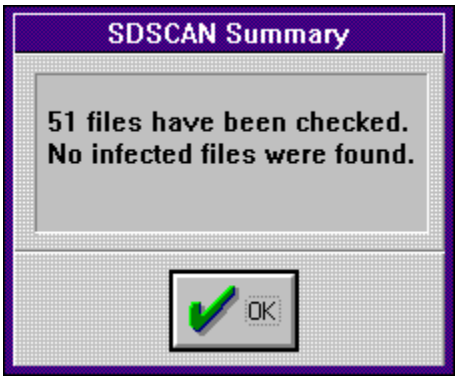
As the scan progresses, a display similar to that shown below will display. The directory tree of the current drive will be displayed as each directories files are being scanned. To the right a listing of all files will display as each file is scanned. The file listing is headed with the word **directory**. Archives such as **.ZIP** or **.ARJ** will be displayed as subdirectories in the directory display. As the files in the archive are decompressed and scanned, their filenames will be displayed in the file list. The archive type will be displayed at the top of the filelist (ie **ZIP Archive**).

An example of the maximized scanning display is shown below.



The scan can be stopped at any time by clicking once on the **Stop Scan** button, or by pressing the **Spacebar** once. A dialog box will be displayed, asking you to confirm your desire to stop the scanning operation. Selecting **OK** will display the summary (below) and return to the Main Panel. Selecting **Cancel** will continue the scan.

Once the scan is complete, a summary box will be displayed, showing the number of files checked and the number of infected files and boot block/partition table viruses found. The number of viruses removed and/or ignored will also be displayed.



When OK is clicked, the Main Panel will again display in the foreground.

VIRUS FOUND!
Scanning While Minimized

Scanning While Minimized

The scan operation can be minimized to an icon. After the scan begins, click on the downward pointing arrowhead at the upper-left corner of the maximized scan display (See Selecting/Deselecting Drives to Scan for an example of this display). The scan will continue in the background, the scan display replaced by one of the two icons above.

The icon is animated, indicating how fast the virus scan is going. Below the icon the current file being scanned will be displayed. Should the icon's movement slow drastically, you should close some applications to free up system resources. Optionally, you may choose to always scan minimized. The scan will become iconized as soon as the scan begins. See SDSCAN Icon Selection for help setting this option.

Regardless of whether minimized manually or as the default scanning option, the scan summary box will be displayed after the scan is complete. Once acknowledged, the Main Panel will be displayed maximized.

Options

The SDSCAN Options Panel

To set permanent options for SDSCAN, from the Main Panel, click on the options button (Shown Above). Keyboard users can select this button with <**Alt-O**>. This panel has a series of selections that will be saved for any future scan. Keyboard users can move the highlight within this panel by using the **Tab** key. The arrow keys may be used to switch between radio buttons, and the **Spacebar** used to select radio buttons and select/deselect check boxes.

Scanning Scope

A virus is harmless unless it is in a form that can be executed by DOS (ie a program file). Such files will have extensions EXE, COM, or SYS. Select the desired scope of the scan operation. Point to the desired Scope and click once. Keyboard users can select the desired scope by using the **right** and l**eft cursor control keys** (**arrow keys**).

If **Program files** is selected for scan scope, then only files with those extensions will be scanned. This will provide you with a rapid and accurate scan of the selected drives.

Archive files will also be included if Scanning Options are set, in which case program files found within supported archives will be scanned also.

If **All Files** is selected as scope, then all files on selected disk/diskette will be scanned. Some viruses can be "hidden" in what looks like a data file, or even cross-linked into an existing data file. This is a rare occurrence, so this selection is not necessary on a routine basis. If you are experiencing symptoms of a virus infection, yet a normal scan detects nothing, you may wish to use this setting.

Scanning Options

There are numerous file compression utilities which are often used to transfer data. It is cumbersome to extract these archives in order to check for viruses. SDSCAN can scan the contents of archives created with ZIP, LHA, or ARJ compression formats.

Select **Archive Files** if you wish the contents of these files to be scanned for viruses or if you are unsure whether such files exist on you system. Click on its checkbox to the left. Keyboard users can toggle this option by pressing **TAB** until the item is outlined, then pressing the **Spacebar** once.

There are some utilities which will compress program files for storage on disk, yet allow them to be expanded into memory in order to execute. This could hide a viruses signature, since when its host is compressed, the viruses own pattern will be altered. SDSCAN can identify and properly scan programs which have been compressed with **Diet**, **LzExe**, and **PkLite**.

Select **Compressed Programs** if you wish these files to be checked if detected. As many commercial software developers are using such utilities, it is suggested that you leave this setting on. To select or deselect this option, point to the checkbox to the left of this selection and click once. Keyboard users can toggle this option by pressing **TAB** until the item is outlined, then pressing the **Spacebar** once.

The SDSCAN Options Panel

When a Virus is Found

You may specify the action that SDSCAN takes when a virus is found on your system. A report is always generated, if a filename is specified in the Reporting section of the Options Panel. Select which of the actions you wish SDSCAN to use as the default by pointing to the desired selection and clicking once. Keyboard users can choose between the desired options by using the **right** and **left cursor control keys** (**arrow keys**).

Prompt: Prompt the user to remove the virus, continue scanning, or abort the scan.
Remove: Remove the virus and continue. The user will be notified.
Report Only: Report to the user that a virus has been detected and what type, but take no other action.

Sample Report

Reporting

You may specify to have a permanent record of scans saved to a text file. Specify a full path and file name of the desired report file, or use the **Browse** button to select a file using a **file selection dialog box**. You may then select the drive and directory as well as the name of an existing or non-existent file (for an example of a **file selection dialog box**, see Scan Menu Commands).

To have all reporting appended to the selected file (if it exists), check off the **Append to Existing Report** box. Point to the check box to the left of the selection and click once. Keyboard users can toggle this selection by pressing **TAB** until the selection is outlined, and pressing the **Spacebar** once. If the file specified does not exist, then the file will be created, regardless of this setting. Should the file exist, then the report will overwrite the existing report.

> **NOTE**: This file is an ASCII text file. It may be viewed using **Notepad** or any similar text file viewer/editor, or imported into word processor applications such as **Microsoft Word for Windows**.

Sample Report

Sample Report:

SDSCAN version 25.05
Licensed Exclusively to Fifth Generation Systems
(c)1991, BRM Technologies

Operation started at: 21-Oct-92 18:44

--- No virus was found in memory ---

Drive A: Boot block
is infected by 'Stoned Virus'.
Note:
Variant number 2.
.
Action:
virus has been ignored.

-- Scanning: A:\ --

------- Summary for drive A: -------
1 boot block virus found.
4 files have been checked.
1 files contain viruses that can be removed.

SDSCAN Icon Selections

While Scanning, SDSCAN can be minimized. This option selects which animated icon you wish to display during a minimized (or iconized) scan. Select the desired icon by pointing to the checkbox to the left of the icon you wish to use and click once. Keyboard users may select the desired icon by using the **right** and **left cursor control keys** (**arrow keys**)

If the **Directory Tree** Icon is selected, the icon has the illusion of a miniaturized version of the directory window displayed during a maximized scan.

When **Sniffy** is selected, **Sniffy** will "Sniff out" any viruses as the files are displayed below the icon.

If the **Scan Iconized** selection box is checked, then SDSCAN will minimize when scanning begins. Toggle this option by pointing to the checkbox to the left of this selection and clicking once. Keyboard users may toggle this option by pressing **TAB** until the option is outlined and pressing the **Spacebar**.
For more information, see Scanning While Minimized

The SDSCAN Options Panel
Selecting/Deselecting Drives to Scan

Menu Command Help

Scan Menu Commands

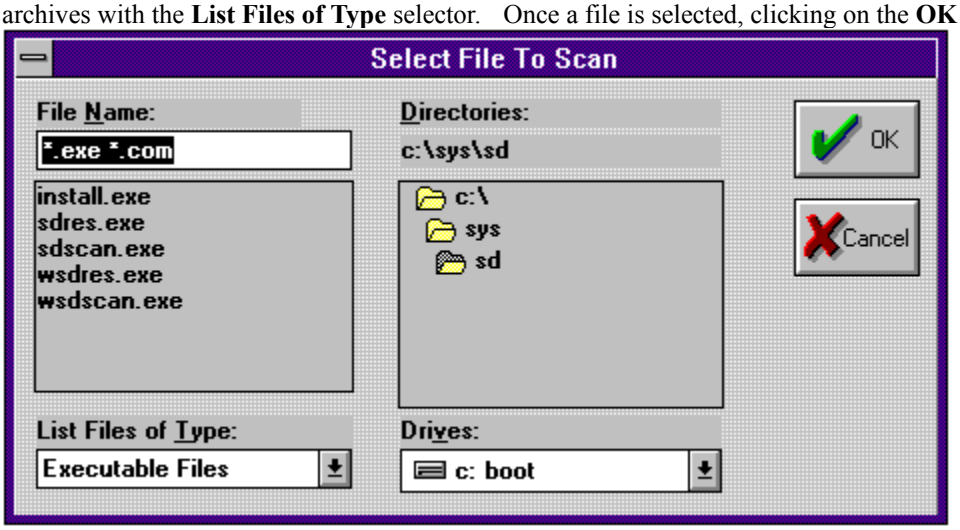
The **Scan** pulldown menu can be accessed by pointing to the word **Scan** on the menu bar on the upper portion of The SDSCAN Main Panel. Keyboard users can access this menu with <**ALT-C**>. Once the menu is pulled down, the individual selections may be highlighted with the arrow keys. **Enter** selects the highlighted item.

Drive(s) :

This selection will begin a scan of the selected drives, scanning all directories. A drive or combination of drives must be selected for this option to function.

File:

This selection is used to scan a single file in a specified drive and directory. A **File Selection Box** will be displayed when the menu item is selected (shown below). The files displayed can be changed from executables to archives with the **List Files of Type** selector. Once a file is selected, clicking on the **OK** button begins the scan.



Exit:

This selection shuts down **SDSCAN**, and closes the Main Panel.

Options Menu Commands

Options Menu Commands

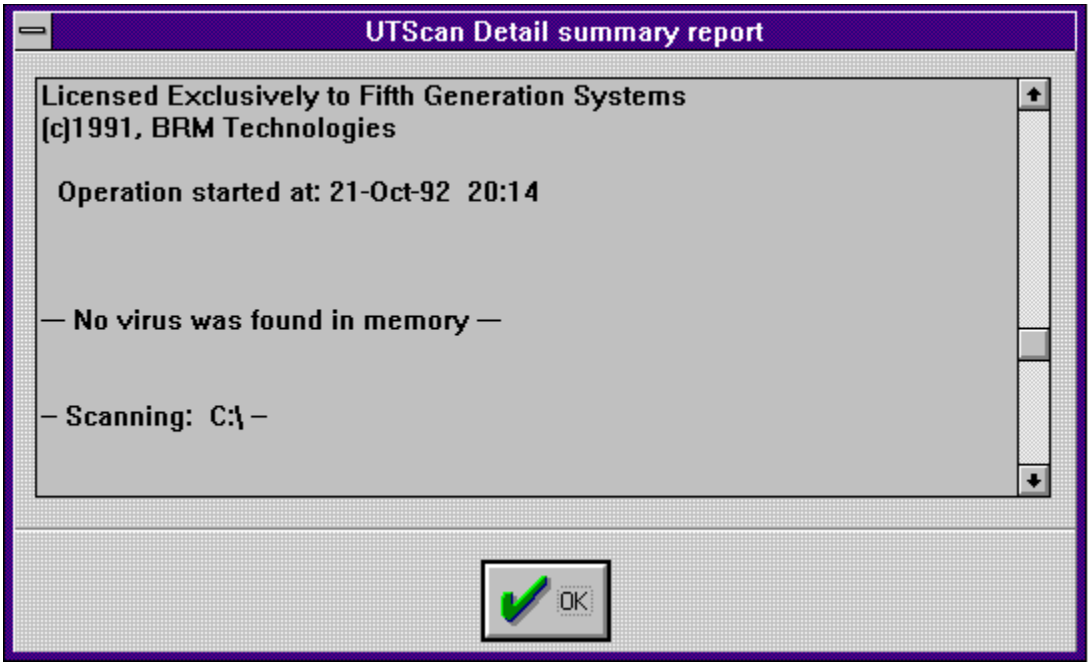
The **Options** pulldown menu can be accessed by pointing to the word **Options** on the menu bar on the upper portion of The SDSCAN Main Panel. Keyboard users can access this menu with <**ALT-O**>. Once the menu is pulled down, the individual selections may be highlighted with the arrow keys. **Enter** selects the highlighted item.

Scanning:

Selecting this menu choice displays The SDSCAN Options Panel.

Report:

This selection displays the report file specified in the Reporting option. An example of the display is shown below:



Help Menu Commands

Help Menu Commands

The **Help** pulldown menu can be accessed by pointing to the word **Help** on the menu bar on the upper portion of The SDSCAN Main Panel. Keyboard users can access this menu with <**ALT-H**>. Once the menu is pulled down, the individual selections may be highlighted with the arrow keys. **Enter** selects the highlighted item.

Contents:
This selection loads **Search & Destroys** Help system and displays the Contents page.

Using Help:
This selection loads **Search & Destroy's** Help system and displays the section on Using this Help System.

About:
This displays Search & Destroy's current signature level and scanner version.

Scan Menu Commands

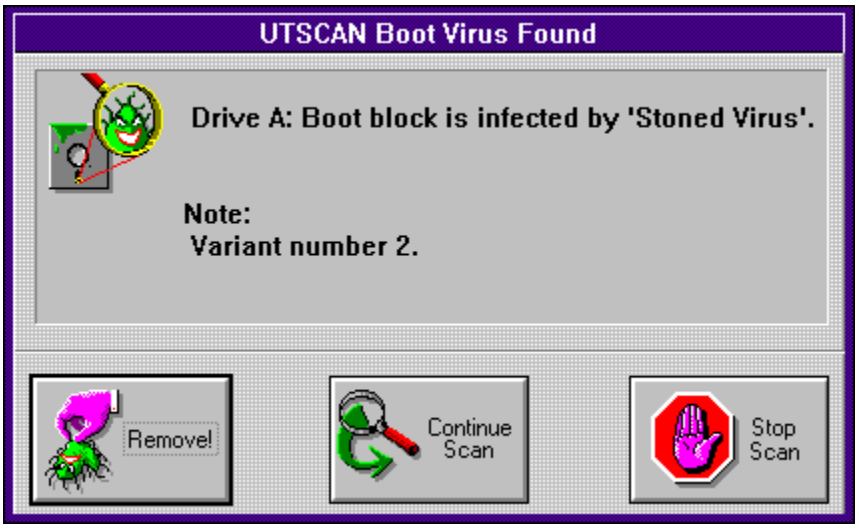
Important Topics

VIRUS FOUND!

If a virus is found on the infected Disk/Diskette, it will be one of two forms, a ***Boot Infector*** or a ***File Infector***. The messages and dialog boxes displayed will be different. Choose the appropriate selection below.

Boot Block Virus Found

If a virus is found in the **Boot Block** of the Disk/Diskette being scanned, a dialog box similar to one shown below will display.



Remove!
Select this if you want SDSCAN to remove the virus from the boot sector. SDSCAN will continue scanning after removing the virus.

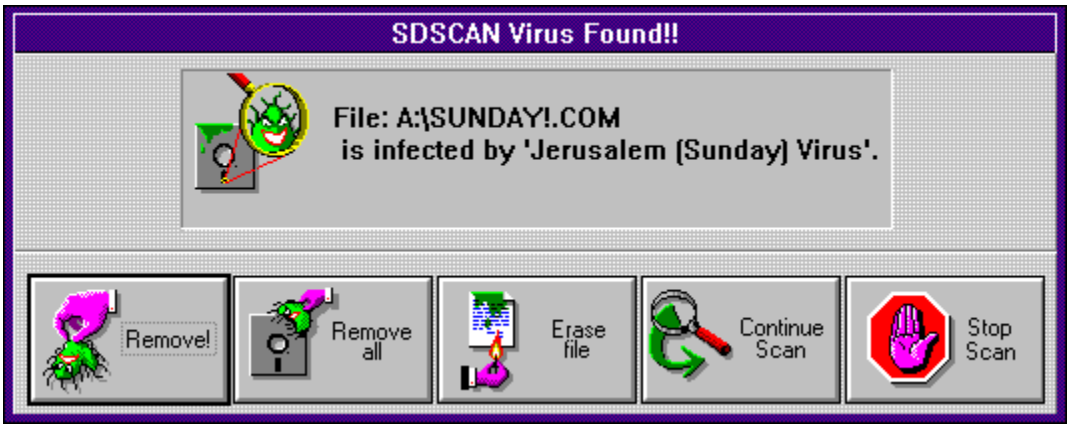
Continue Scanning
Select this if you wish to leave the virus and continue scanning.

Stop Scan
Select this to abort the current scan. The SDSCAN Main Panel will display after the scan summary.

Getting Technical Support
Using the Virus Listing
Virus Types

File Infector Virus Found

If a file being scanned is found to be infected with a Virus then a dialog box similar to one shown below will be displayed.



Remove!
Select this to remove the virus from the file and continue the scan. Prompt any other virus detected.
Remove all
Select this to remove the virus. Continue the scan and remove any other viruses found.
Erase File
Select this to erase the infected file. Continue the scan, prompt if viruses found.
Continue Scanning
Skip this file and continue scanning. Prompt if viruses found.
Stop Scan
Abort the scan and return to the SDSCAN Main Panel.

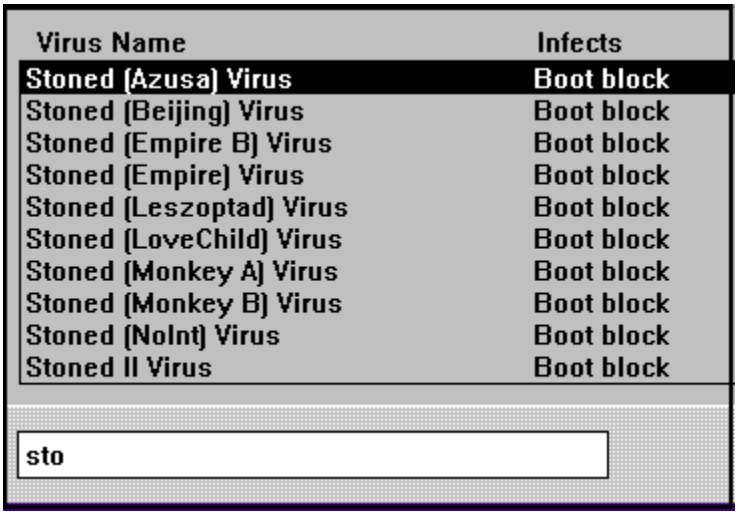
Using the Virus Listing
Getting Technical Support
Virus Types

Using the Virus Listing

An alphabetical listing of the viruses which SDSCAN can remove is available from the SDSCAN Main Panel. A window displays a list of Virus names and the Virus Type

Below the display is an empty field which can be used to perform an instant keyword search. As a word is typed, the listing is rapidly searched for the keyword until enough characters are typed for the desired virus name to be found.

For Example, if you wish to see if your version of Search & Destroy can detect the Stoned Virus, first call up the virus listing. Start typing S-T-O. When enough characters have been typed to identify the name, that portion of the virus listing will be displayed.



A Little About VIRUSES
Tips

Uninstalling Search & Destroy
Upgrading to Untouchable

If you have purchased Fifth Generation Systems **Untouchable** anti virus system, and need to install it to your computer, it will first be necessary to uninstall Search & Destroy. Should you wish to uninstall for any reason, follow these steps.

First exit Windows by selecting **Exit** from the **File** Menu in program manager (Consult your documentation if you are using a third party Windows shell such as **Direct Access Desktop**).

From the DOS prompt, log to the drive and directory where Search & Destroy's files are installed. (User Input shown in bold)

C:\> **cd \sd <ENTER>**
C:\SD>**install <ENTER>**

Search and Destroy's install menu will be displayed. You will be given the options
Automatic Install
Manual Install

Quit

Select Manual Install.
Another Menu will be displayed, showing the installation steps:

Scan for known virus signatures
Install Search & Destroy on hard disk
Install Windows version.

Uninstall.

Quit

Select **U**ninstall. The DOS and Windows version will be uninstalled. The **M**anual Install menu will be displayed.
Select **Q**uit from the **M**anual Install menu. The main menu will be displayed.

Select **Q**uit from Search and Destroy's Install main menu.

You are now ready to install Untouchable. Consult the **Getting Started** instructions provided with **Untouchable** for instructions on install.

Getting Technical Support

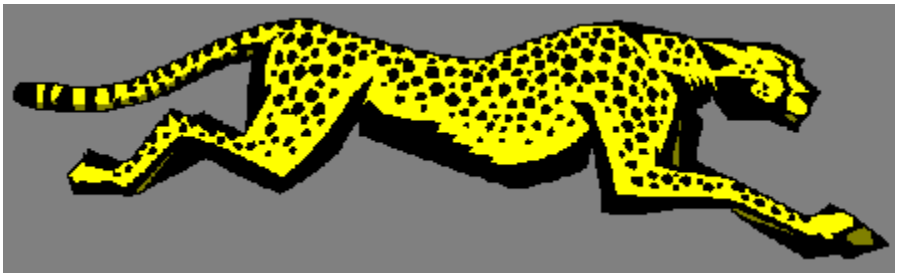
Tips

Here are a few tips to help establish good practices for virus prevention.

Keep a write protected Boot Diskette handy with SDSCAN.EXE on it. Consult your DOS users manual for instructions on creating a boot diskette.
Always inspect and Scan new diskettes before using them. This should include even diskettes from software packages purchased at dealers
Do Not Use hacked or pirated software. These can be infected with viruses either purposely or inadvertently. As it is exchanged from user to user, the opportunities for infections increase.
Keep an up to date backup of your files. A product such as **Fastback Plus** is an example of a utility to do this, available in a windows or DOS version.
Use a security oriented menuing system or shell. **Direct Access** or **Disklock for the PC** for example.
Be Wary. Take note of any bizarre or unexplained behavior. There is always a reason.

A Little About VIRUSES
Symptoms
Getting Technical Support

Fifth Generation Systems, Inc.



Main Address

Fifth Generation Systems
10049 N. Reiger Rd
Baton Rouge, LA 70809-4559
Business phone: 1-504-291-7221
Fax: 1-504-295-3268
Sales Phone: 1-800-873-4384

Hong Kong

FGS Hong Kong, Ltd
3715 Sun Hung Kai Centre
30 Harbour Rd.
Wanchai, Hong Kong
Business phone: 852-827-6977
Fax: 852-824-3200

Europe

Fifth Generation Systems, Ltd.
Cliveden Office Village
Lancaster Road, High Wycombe
Bucks, HP12 3YZ, England
Business Phone: 44-(0)-494-442224
Fax: 44-(0)-494-442225
Sales/Support: 44-(0)-494-442223
(Note: 0's are only needed within the UK)

Getting Technical Support

Fifth Generation Systems
Technical Support
24 Hours a Day
7 Days a Week

Fifth Generation Systems supplies 24-hour Technical Assistance by phone for its customers throughout the world.

Technical Support / Customer Service

Phone: 1-800-766-7283 (Toll Free from U.S.A., Canada, Puerto Rico)
1-504-291-7283
Fax: 1-504-295-3268

BBS:
1-504-295-3344 (1200/2400, 8,N,1)
1-504-295-3225 (1200/2400, 8,N,1)
1-504-295-3065 (1200/2400, 8,N,1)
1-504-295-3261 (9600/14400, 8,N,1 Supra Faxmodem v.32/v.32bis)

Compuserve Forum: GO FIFTH

Internet Address: 75300.3663 @ COMPUSERVE.COM

International 800 Support Numbers

Malaysia:	800-2387
Australia:	0014-800-128-463
Indonesia:	00-800-011-0204
New Zealand:	0800-447882
Singapore:	800-7780
Japan:	0031-12-3241
Korea:	008-14-800-0207
Hong Kong:	800-5835
Taiwan:	0080-13-8245
Thailand:	001-800-12-066-0162

Index of Topics