Help index

General

Menu

Check

Setup

Log

Pop-up windows

Help for IBM AntiVirus/DOS

IBM AntiVirus/DOS can prevent, detect and remove computer viruses. It can work in the background, providing constant protection for your system. You can also use it directly to check diskettes or hard disks for viruses.

Use the main window of IBM AntiVirus/DOS to check your system for viruses now, to check a diskette for viruses, to configure the way in which your system is checked, to view logs generated during checks, or to view online help.

When you have configured IBM AntiVirus/DOS to perform an automated check of your system, it is not usually necessary to check it yourself in this way.

Additional help is available for:

Push here push button
Check
Setup
Log
Help

Help for Push here

Use the **Push here** push button on the main window to check your system for viruses now. The settings that are used can be seen by selecting the **Check system** menu item from the **Check** menu. When you have configured IBM AntiVirus/DOS to perform an automated check of your system, it is not usually necessary to check it yourself in this way.

Help for Check

Use the menu items on the **Check** menu to check a diskette for viruses, to check your system for viruses, or to exit IBM AntiVirus/DOS. The **Check diskettes** and **Check system** menu items also allow you to configure the way these checks are done.

Additional help is available for:

Check diskettes
Check system
Exit

Help for Check diskettes choice

Use **Check diskettes** to check a diskette for viruses and to configure the way this checking is done.

Help for Check system choice

Use **Check system** to check your system for viruses and to configure the way this checking is done. The configuration defined by **Check system** is also used when the **Push here** push button is selected from the main window.

Help for Exit

Use **Exit** to close the IBM AntiVirus/DOS application. Any automated checking or DOS shielding that has been set up is still in effect even if you close IBM AntiVirus/DOS.

Help for Setup

Use the menu items on the **Setup** menu to configure IBM AntiVirus/DOS. You can set up automated checking so you do not have to remember to check your system yourself. You can also tell IBM AntiVirus/DOS to shield DOS so that common viruses cannot spread on your system.

Additional help is available for:

Automated check
Shield DOS

Help for Automated check choice

Use **Automated check** to set up automated checking of your system for viruses or to turn off automated checking. You can also configure the way this checking is done. When you have configured IBM AntiVirus/DOS to perform an automated check of your system, it is not usually necessary to check the system yourself. This is the recommended way of configuring IBM AntiVirus/DOS.

Help for Shield DOS choice

Use **Shield DOS** to tell IBM AntiVirus/DOS to prevent common viruses from spreading from within DOS. You can also tell IBM AntiVirus/DOS not to shield DOS. Using this feature to shield DOS is the recommended way of configuring IBM AntiVirus/DOS.

Help for Log

Use the menu items on the **Log** menu to view logs about checks for viruses.

Additional help is available for:

Current log
Previous log
Cumulative log

Help for Current log

Use the **Current log** menu item to view the log of virus checks generated from your current IBM AntiVirus/DOS session.

The current log is kept in the file CURRENT.LOG in the directory where IBM AntiVirus/DOS was installed. This is a normal file that can be printed directly on your printer.

Help for Previous log

Use the **Previous log** menu item to view the log of virus check information generated from your previous IBM AntiVirus/DOS session.

The previous log is kept in the file PREVIOUS.LOG This is a normal file that can be printed directly on your printer.

Help for Cumulative log

Use the **Cumulative log** menu item to view the cumulative log of automated virus check information generated by IBM AntiVirus/DOS. Use this option to verify that automated checks were done as expected and to review whether any viruses were found.

The cumulative log is kept in the file CUM.LOG in the directory where IBM AntiVirus/DOS was installed. This is a normal file that can be printed directly on your printer. An entry is added to the cumulative log each time IBM AntiVirus/DOS does an automated check. It does not record checks that you do manually. You can edit or erase this log file if it grows too large.

Help for Help

Use the menu items on the **Help** menu to view the online help for IBM AntiVirus/DOS.

Additional help is available for:

Help index
General help
Using help
Keys help
Virus descriptions
Contacts
Product information

Help for Help index

Use **Help index** to see an index of all the online help for IBM AntiVirus/DOS.

Help for General help

Use **General help** to see introductory help information for IBM AntiVirus/DOS. More detailed contextual help is always available by pressing F1.

Help for Using help

The **Using help** menu item explains how to use the online help system.

Help for Keys help

Use **Keys help** to view a list of keys that you can use to perform various actions within IBM AntiVirus/DOS. These keys can be used instead of selecting menu items.

Help for About Viruses

Use **About Viruses** to view general information about viruses. The information provided includes an introduction to computer viruses, and discusses techniques used by anti-virus programs, including IBM AntiVirus/DOS.

Help for Virus descriptions

Use **Virus descriptions** to view descriptions of many of the viruses that have been analyzed by IBM. These many viruses include all of the viruses that are widespread in the world as of this writing. It also includes many viruses that are not widespread but that IBM has analyzed to stay ahead of the problem.

Virus descriptions also gives a list of the known DOS viruses that IBM AntiVirus/DOS detects.

Help for Contacts choice

Use **Contacts** to view a list of contacts from whom assistance is available. This list can be modified to include local contacts by editing the file CONTACT.LST that is distributed along with IBM AntiVirus/DOS. The file CONTACT.LST is in the same directory that contains the files for IBM AntiVirus/DOS.

Help for Product information

The **Product information** menu item allows you to view information about IBM AntiVirus/DOS, such as the version number.

Help for Check diskettes window

Use **Check diskettes** to check a diskette for viruses, and to change the way this checking is done. Select the diskette you want to check from the **Diskette** selection box, choose whether to check program files or all files, then select the **Execute** push button.

Additional help is available for:

Diskette selection box
Files to check
Save settings
Execute
Cancel

Help for Diskette selection box

Scroll the **Diskette** selection box display until the diskette drive that you want to check is visible, then select the diskette drive.

Help for Files to check on diskette

You can select whether program files or all files are to be checked. Selecting **Program files** tells IBM AntiVirus/DOS to check files on the diskette that are normally executable. These are files that have file types of BAT, BIN, CMD, COM, DOS, DLL, EXE, OS2, OV?, PRG and SYS. Selecting **All files** tells IBM AntiVirus/DOS to check all files on the diskette. The boot record of the diskette is checked for viruses in either case.

Normally, viruses only infect program files. Checking program files is the correct thing to do in most cases. The only exceptions are if an executable file has been renamed to some other file type or if a program uses overlay files that have some other file type. Usually, files other than program files are data files that do not become infected with viruses. Checking all files finds viruses, no matter what files they are in, but it takes longer because more files need to be checked.

Help for Check diskettes Save settings

Use **Save settings** to save the settings that you have specified (which diskette drive to check, and which files are to be checked). When you select the **Check diskettes** menu item at a later time, these saved settings are displayed.

Help for Check diskettes Execute

Selecting the **Execute** push button checks the diskette in the specified drive for viruses now. The files checked are the ones that you have specified in the **Files to check** box. If a virus is found on a diskette, you will be given the option to remove the virus or erase the file. Once checking is completed on one diskette, you are given the option of checking another diskette.

Help for Check diskettes Cancel

Selecting the **Cancel** push button closes the **Check diskettes** pop-up window and returns you to the previous window. When you select the **Cancel** push button, any settings on this pop-up window that you have not saved are discarded.

Help for Checking for viruses

The **Checking for viruses** pop-up window is displayed when IBM AntiVirus/DOS is checking your system for viruses. A progress bar shows the percentage of which the check is complete. The name of the current file being checked is displayed. When checking is complete, you see a display indicating whether or not a virus has been found. If a virus is found, you will be given the option to remove the virus.

Additional help is available for:

Stop

Help for Stop

Use the **Stop** push button to end this check. You are asked to confirm the stop request. If you confirm by selecting **Yes**, checking will stop, and the log will be updated for the checks that have been completed. Checking stops after the current file is finished so there might be a slight delay. If an indication of a virus has been detected the **Virus infection report** pop-up window will be displayed.

Help for Check system window

The **Check system** pop-up window allows you to check your system's drives (both local and LAN attached) for viruses and to change the way this check is done. If a virus is found during this check, you will be given the option to remove it.

Select the drives to check, the files to check, and in which files to look for known viruses. Then select **Execute** to perform the check.

If the **Advanced options selected** check box is checked, the **Drives to check** and **Files to check** information is taken from the **Advanced options** settings.

Additional help is available for:

Drives to check
Files to check
Look for known viruses in
Advanced options
Default settings
Save settings
Execute
Cancel

Help for Drives to check

You can select the drives to be checked for viruses. If you select **Fixed drives,** all of the local fixed drives on your system will be checked. If you select **Network drives,** all network-based server drives to which you are linked will be checked. All directories on the specified drives are checked. When you want to check some other combination of drives or directories, you must specify them by selecting the **Advanced options** push button. You must specify at least one drive to check, either by selecting **Fixed drives, Network drives,** or by selecting drives using **Advanced options.**

Usually, you want to check all local fixed drives to determine if there is a virus on your own system. You do not usually want to check all network drives. Because network drives tend to have a large number of files, checking them can take a substantial amount of time. If several systems on the network are checking all network drives, it will reduce the performance of these drives for other network users. When network drives are checked, they should usually be checked by only one system and only when the network usage is low.

Help for Files to check on system

You can select whether program files or all files are to be checked. Selecting **Program files** tells IBM AntiVirus/DOS to check files that are normally executable on the specified drives. These are files that have file types of BAT, BIN, CMD, COM, DOS, DLL, EXE, OS2, OV?, PRG and SYS. Selecting **All files** tells IBM AntiVirus/DOS to check all files on the specified drives. In either case, the master boot record and all active partition boot records on any specified local, fixed drive are also checked, including Boot Manager boot records. When a file cannot be accessed for some reason, it is skipped and checking continues.

Normally, viruses only infect program files. Checking program files is the correct thing to do in most cases. The only exceptions are if an executable file has been renamed to some other file type or if a program uses overlay files that have some other file type. Usually, files other than program files are data files that do not become infected with viruses. Checking all files finds viruses, no matter what files they are in, but it takes longer because more files need to be checked.

Help for Look for known viruses in

IBM AntiVirus/DOS checks several features of boot records and files to determine if they are infected. One of these checks is to scan the boot record or file for known viruses. You can select whether IBM AntiVirus/DOS scans all specified files and boots records for viruses or only scans those that have changed or are new since the last check. Boot records and files that you have specified are always checked for other features, even if you choose not to scan those that have not changed.

If you select **Only new/changed files,** files and boot records are checked to see if they are new or changed and are only scanned for known viruses if they are. Viruses must change the boot records and files they infect in order to infect them. Because there were no viruses the last time a check was performed, the only boot records or files that can be infected now are those that have changed. Checking only those that have changed is usually the correct thing to do.

If you select **Even unchanged files,** all specified files and boot records are scanned, whether they have changed or not. This takes substantially longer than selecting **Only new/changed files.**

Help for Advanced options choice

Use **Advanced options** to select more complex combinations of drives or files to check. If the **Selected** check box is checked, advanced options are in effect. In this case, the drives and files to check are specified on the **Advanced options** pop-up window, rather than on the **Check system** pop-up window.

To choose advanced options, select the **Advanced options** push button. To deselect advanced options, uncheck the **Selected** check box in the **Check system** pop-up window.

Help for Check system Default settings

Selecting the **Default settings** push button returns the settings on the **Check system** pop-up window to their default and recommended values. Any other values that had been specified are discarded.

The **Save settings** push button needs to be selected to save the default settings for subsequent IBM AntiVirus/DOS sessions.

Help for Check system Save settings

Selecting the **Save settings** push button saves the settings on the **Check system** pop-up window. When you select the **Check system** menu item at a later time, these saved settings are used.

Help for Check system Execute

Select the **Execute** push button to check the specified drives for viruses now. The files that are checked are the ones that you have specified in the **Files to check** box. If a virus is found on any of the selected disks, you will be given the option to remove the virus and to do a more thorough search to make sure all instances of the virus are eliminated.

Help for Check system Cancel

Use **Cancel** to close the **Check system** pop-up window and to return to the previous window. When you select the **Cancel** push button, any settings on this pop-up window that you have not saved are discarded.

Help for Advanced options window

The **Advanced options** pop-up window allows you to specify more complex combinations of drives, subdirectories, and files to be checked for viruses than does the **Check system** pop-up window. The **Advanced options** pop-up window is accessed by selecting the **Advanced options** push button on the **Check system** pop-up window.

Select the drive, directory, and files you want to check. Then use the **Add** push button to add them to the **Paths selected for checking** box. Repeat this process until everything that you want to check is listed in the **Paths selected for checking** selection box. Use the **Save settings** push button if you want to save these settings permanently. Then use the **Execute** push button to perform the check.

Note that only items that appear in the **Paths selected for checking** selection box are used during this check. The only way to put items in the **Paths selected for checking** selection box is with the **Add** push button.

Additional help is available for:

- **Drives/Directories**
- **Files to check**
- **Paths selected for checking**
- **Add**
- **Delete**
- **Default settings**
- **Save settings**
- **Execute**
- **Cancel**

Help for Drives/Directories

Use the **Drives/Directories** selection boxes to select a drive and directory to check. The files to check on that drive and directory are selected with the **Files to check** box.

Note that you must use the **Add** push button to add a selected item to the **Paths selected for checking** selection box in order for it to be checked.

Help for Files to check

Use the **Files to check** box to select the files to check on the specified drive and directory.

Selecting **Program files** tells IBM AntiVirus/DOS to check files that are normally executable on the specified drive and directory. These are files that have file types of BAT, BIN, CMD, COM, DOS, DLL, EXE, OS2, OV?, PRG and SYS. Selecting **All files** tells IBM AntiVirus/DOS to check all files on the specified drive and directory. In either case, the master boot record and all active partition boot records on the specified drive are also checked if the drive is a local hard disk, including Boot Manager boot records.

Normally, viruses only infect program files. Checking program files is the correct thing to do in most cases. The only exceptions are if an executable file has been renamed to some other file type or if a program uses overlay files that have some other file type. Usually, files other than program files are data files that do not become infected with viruses. Checking all files finds viruses, no matter what files they are in, but it takes longer because more files need to be checked.

Selecting **Specific files** allows you to specify a particular file in the selection box below. The selection box displays the files in the selected drive and directory. Select the files that you want to check, and select the **Add** push button in the **Paths selected for checking** selection box to add them to the list.

Note that you must use the **Add** push button to add a selected item to the **Paths selected for checking** selection box for it to be checked.

If a file cannot be accessed for some reason, it is skipped and checking continues.

Help for Paths selected for checking

When you have specified the drive, directory, and files that you want to check, add them to the list by selecting the **Add** push button. You can delete items from the list by selecting them, then selecting the **Delete** push button. When the **Paths selected for checking** box lists everything you want to check, select the **Execute** push button to perform the check.

Note that you must use the **Add** push button to add a selected item to the **Paths selected for checking** selection box in order to check it.

Help for Add

Use the **Add** push button to add the specified drive, directory, and files to the list of files to check.

Note that you must use the **Add** push button to add a selected item to the **Paths selected for checking** selection box in order to check it.

Help for Delete

Use the **Delete** push button to delete the selected items from the list of files to check in **Paths selected for checking.**

Help for Advanced options Default settings

Use the **Default settings** push button to return the settings on the **Advanced options** pop-up window to their default and recommended values. Any other values that had been specified are discarded.

The **Save settings** push button needs to be selected to save the default settings for subsequent sessions.

Help for Advanced options Save settings

Use the **Save settings** push button to save the settings on the **Advanced options** pop-up window. When you select **Advanced options** at a later time, these saved settings are used.

Help for Advanced options Execute

Use the **Execute** push button to check the specified list of drives, directories, and files for viruses now. If a virus is found, you will be given the option to remove the virus and to do a more thorough search to make sure all instances of the virus are eliminated.

Note that you must use the **Add** push button to add a selected item to the **Paths selected for checking** selection box for it to be used for this check.

Help for Advanced options Cancel

Use the **Cancel** push button to close the Advanced Options pop-up window and return to the previous pop-up window. When you select the **Cancel** push button, any settings on this pop-up window that you have not saved are discarded.

Help for Virus infection report

The **Virus infection report** pop-up window displays when IBM AntiVirus/DOS has found a possible virus on your system or on a diskette. Boot records and files that might contain a virus are listed according to how certain it is that they are infected.

You should examine the lists carefully and disinfect or erase anything that is infected. If you do not disinfect or erase infected items, it is very likely that the infection will continue to spread on your system and perhaps to other systems as well.

Note that files that are erased cannot be recovered (not even with unerase utilities).

Names of files that you erase are written to the log to help you restore them from backups if necessary. To view the log, select either **Current log** or **Previous log** from the **Log** menu on the main window.

Occasionally, it might not be possible either to disinfect, or to erase or replace a file or boot record because the system does not allow it to be altered. This problem might occur if the operating system has locked the file or if a security system you are using does not give you write access to the file or boot record. Consult the documentation for your operating system, security system, and so forth for information on unlocking these files or boot records. Alternatively, you might be able to start your system from a diskette and use the IBM AntiVirus/DOS stand-alone program to disinfect or erase these files or boot records.

Additional help is available for:

Definite
Probable
Suspicious
OK
Cancel

Help for Definite

Boot records and files listed in the **Definite** selection box are definitely infected with the virus shown. IBM AntiVirus/DOS has verified that each relevant piece of the virus is identical to the standard virus in IBM's collection. This verification ensures that it is safe to disinfect it. Disinfection is normally the correct thing to do, because it removes the virus and restores each boot record or file to its original, uninfected state.

Initially, all items on this list are selected. All you have to do is to select the **Disinfect** radio button, and then select the **OK** push button to disinfect them.

See the additional help for **Erase/Replace** before erasing anything. Note that files that are erased cannot be recovered (not even with unerase utilities).

Additional help is available for:

Disinfect
Erase/Replace
Select all
Deselect all

Help for Disinfect

Use **Disinfect** to remove the virus from the selected items and restore them to their original, uninfected state.

While the Windows portion of IBM AntiVirus/DOS correctly detects infected diskettes, it is not always able to disinfect them.   If you find you have infected diskettes, we recommend that you invoke the DOS portion of the product by going to a DOS prompt, changing to the directory where IBM AntiVirus/DOS is installed, and issuing the command IBMAVD.

Help for Erase/Replace in Definite box

Use **Erase/Replace** to overwrite and erase the selected items.

Initially, all items on this list are selected. All you have to do is ensure that the **Erase/Replace** check box is checked, and select the **OK** push button to erase files or replace boot records.

When you use this feature to "erase" files, the files are first overwritten and then deleted. This operation prevents infected files from being accidentally restored with "unerase" utilities. Files that are erased in this way cannot be recovered (not even with unerase utilities).

Names of files that you erase are written to the log to help you restore them from backups if necessary. To view the log, select either **Current log** or **Previous log** from the **Log** menu on the main window.

"Replacing" the master boot record of a hard disk replaces it with a valid master boot record, which is normally the correct thing to do if they cannot be disinfected. The only exception is when the hard disk had an unusual master boot record similar to those used by some DOS security products. In these cases, "replacing" the master boot record might leave the system in an unusable state. Contact the vendor of the security product for assistance before trying to remove the virus from these systems.

Erase/Replace cannot be used to overwrite system boot records, including Boot Manager boot records, because their format depends on the particular version of the operating system that you are using.

Help for Select all in Definite box

Use **Select all** to select all of the items in the **Definite** selection box. You can then use **Disinfect** or **Erase/Replace** to disinfect or erase them all.

Help for Deselect all in Definite box

Use **Deselect all** to deselect all of the items in the **Definite** selection box. You can then select them individually and disinfect or erase them.

Help for Probable

Boot records and files listed in the **Probable** selection box have a pattern of bytes similar to a pattern found in the standard virus in IBM's collection. As a result, they are probably infected with the virus shown or a virus closely related to it. It is not possible for IBM AntiVirus/DOS to determine that the virus is absolutely identical to the standard virus in IBM's collection. As a result, attempting to remove the virus by disinfection might result in a damaged boot record or file. The correct action to take is almost always to "erase/replace" the infected objects. Infected files can then be replaced from backups or write-protected original diskettes.

Initially, all items on this list are selected. All you have to do is ensure that the **Erase/Replace** check box is checked, and select the **OK** push button to erase files or replace boot records.

See the additional help for **Erase/Replace** before erasing anything. Note that files that are erased cannot be recovered (not even with unerase utilities).

Note that some other anti-virus programs can sometimes be identified as "probably infected", because those programs do not use the recommended industry techniques to avoid misleading identification. Contact the vendor of the other anti-virus program for assistance.

Additional help is available for:

Erase/Replace
Select all
Deselect all

Help for Erase/Replace in Probable box

Use **Erase/Replace** to overwrite and erase the selected items.

Initially, all items in the selection box are selected. All you have to do is ensure that the **Erase/Replace** check box is checked, and select the **OK** push button to erase files or replace boot records.

When you use this feature to "erase" files, the files are first overwritten, then deleted. This operation prevents infected files from being accidentally restored with "unerase" utilities. As a result, files that are erased in this way cannot be recovered (not even with unerase utilities).

Names of files that you erase are written to the log to help you in restoring them from backups if necessary. To view the log, select either **Current log** or **Previous log** from the **Log** menu on the main window.

"Replacing" the master boot record of a hard disk replaces it with a valid master boot record. This replacement is almost always the right thing to do. The only exceptions are when the hard disk had an unusual master boot record, similar to those used by some DOS security products. In these cases, "replacing" the master boot record might leave the system in an unusable state. Contact the vendor of the security product for assistance before trying to remove the virus from these systems.

Erase/Replace cannot be used to overwrite system boot records because their format depends on the particular version of the operating system that you are using, including Boot Manager boot records.

Help for Select all in Probable box

Use **Select all** to select all of the items in the **Probable** selection box. You can then use **Erase/Replace** to erase them all.

Help for Deselect all in Probable box

Use **Deselect all** to deselect all of the items in the **Probable** selection box. You can then select and erase them individually.

Help for Suspicious

Files listed in the **Suspicious** selection box have unusual properties or changes that are typical of virus infections. They are not infected with any virus that IBM AntiVirus/DOS knows about.

IBM AntiVirus/DOS does not list boot records or files here just because they have changed. Boot records and files change on computers all the time for reasons unrelated to viruses. IBM AntiVirus/DOS only reports files as "suspicious" if their pattern of change is typical of virus infections.

You should examine the items in this list to determine if there is a good reason for them to have changed recently, other than a virus. One possible reason would be if these files were modified by some other anti-virus program to "inoculate" them. Another reason would be if you recently updated these files, and you are absolutely certain that the updates are not infected.

If you conclude that the files might be infected, the best thing to do is erase them and replace them from backups or write-protected, original diskettes.

Initially, no items in the selection box are selected. You should select the files you want to erase or the boot records you want to replace. Then ensure that the **Erase/Replace** check box is checked, and select the **OK** push button to erase files or replace boot records.

See the additional help for **Erase/Replace** before erasing anything. Note that files that are erased cannot be recovered (not even with unerase utilities).

Additional help is available for:

Erase/Replace
Select all
Deselect all

Help for Erase/Replace in Suspicious box

Use **Erase/Replace** to overwrite and erase the selected items.

Initially, no items in the selection box are selected. You should select the files you want to erase or the boot records you want to replace. Then ensure that the **Erase/Replace** check box is checked, and select the **OK** push button to erase files or replace boot records.

When you use this feature to "erase" files, the files are first overwritten and then deleted. This operation prevents infected files from being accidentally restored with "unerase" utilities. As a result, files that are erased in this way cannot be recovered (not even with unerase utilities).

Names of files that you erase are written to the log to help you restore them from backups if necessary. To view the log, select either **Current log** or **Previous log** from the **Log** menu on the main window.

"Replacing" the master boot record of a hard disk replaces it with a valid master boot record. This replacement is almost always the right thing to do. The only exceptions are when the hard disk had an unusual master boot record, similar to those used by some DOS security products. In these cases, "replacing" the master boot record might leave the system in an unusable state. Contact the vendor of the security product for assistance before trying to remove the virus from these systems.

Erase/Replace cannot be used to overwrite system boot records or Boot Manager boot records because their format depends on the particular version of the operating system that you are using,

Help for Select all in Suspicious box

Use **Select all** to select all of the items in the **Suspicious** selection box. You can then use **Erase/Replace** to erase them all.

Help for Deselect all in Suspicious box

Use **Deselect all** to deselect all of the items in the **Suspicious** selection box. You can then select and erase them individually.

Help for Virus infection report OK

Use **OK** to clean up the items that you have selected in the **Virus infection report** window. If you have selected **Disinfect,** the file or boot sectors that you have selected in the **Verified** list box will be disinfected. If you have selected **Erase/Replace,** files that you have selected in that list box will be erased, and boot sectors will be replaced.

See the additional help for **Erase/Replace** before erasing anything. Note that files that are erased cannot be recovered (not even with unerase utilities).

Help for Virus infection report Cancel

Use **Cancel** to close the **Virus infection report** window and return to the previous window. Any infected files or boot sectors that are still present in the list boxes will not be cleaned up.

Help for Local data

The **Local data** pop-up window provides information or instructions on virus incident handling procedures.

If the file LOCAL.MSG is present in the same directory as IBM AntiVirus/DOS, its contents are displayed in this pop-up window when viruses are found on the system. Only the first 512 bytes of LOCAL.MSG are used by the IBM AntiVirus/DOS DOS Shield program. The other parts of IBM AntiVirus/DOS use the entire LOCAL.MSG file.

Additional help is available for:

Cancel

Help for Local data Cancel

Use the **Cancel** push button to close the **Local data** pop-up window.

Help for Automated check window

The **Automated check** pop-up window lets you configure IBM AntiVirus/DOS to perform an automated check of your system, so that you do not need to check it yourself IBM AntiVirus/DOS should normally be configured to perform this automated check.

Using radio buttons, select when you want the automated check to be done. Select **Save settings** to save these settings.

You can then select **Check options** to specify the way the check is done. When you are finished, use **Cancel** to exit this pop-up window.

Additional help is available for:

Radio buttons
Check options
Save settings
Cancel

Help for Radio buttons

You can tell IBM AntiVirus/DOS to check your system for viruses when you start your system.

Specifying **Every boot** checks your system whenever it is started from the hard disk. If you frequently start your system from diskettes, it might become infected with a boot sector virus from one of these diskettes. Setting up an automated check when your system starts up from the hard disk allows you to check for this possibility whenever you start up.

Selecting **Daily** checks your system every day when you first start up.

Selecting **Monthly** checks your system on the first startup of each month.

Selecting **Weekly** checks your system on the first startup of each week. Note that a week always starts on Sunday.

Selecting **Never** never checks your system automatically.

If your system is not started when the check was scheduled to occur, it is done the next time your system is started.

Help for Check options

Selecting the **Check options** push button opens the **Check system** pop-up window and allows you to specify what disks and files are examined during the automated check.

Help for Automated check Save settings

Selecting the **Save settings** push button saves the settings on the **Automated check** pop-up window, as well as the settings you have specified as **Check options.** When the automated check is performed, these saved settings are used.

Help for Automated check Cancel

Use **Cancel** to close the **Automated check** pop-up window and return to the previous window. When you select the **Cancel** push button, any settings on this pop-up window that you have not saved are discarded.

Help for Shield DOS window

Use the **Shield DOS** pop-up window to prevent common DOS viruses from spreading on your system.

To view the list of viruses that IBM AntiVirus/DOS knows about, select **Virus descriptions** from the **Help** menu on the main window. Then select **List of viruses detected by IBM AntiVirus/DOS** from the help screen. Viruses that are prevented by the shield are marked on this list.

This is a very important feature. Some common viruses corrupt programs in such a way that it might not be possible to disinfect them reliably. Such programs, including IBM AntiVirus/DOS, might not function correctly and might need to be reinstalled if they become corrupted in this way. Keeping the DOS shield installed at all times helps prevent this from happening.

If you check **Install shield,** the shielding program will be loaded whenever DOS is started in the future. The DOS memory space is checked for resident viruses when DOS is started. Subsequently, the shielding program monitors activity in DOS for indications of activity from common DOS viruses. If viral activity is found, you will see a warning. The virus is not allowed to become active or to spread, and you can use the infected program as if it were not infected.

If you uncheck **Install shield,** the shielding program will not be installed when DOS is started in the future.

Normally, IBM AntiVirus/DOS checks high memory (memory above the 640KB DOS limit) for resident viruses. This check might cause problems on some systems, especially where hardware adapters are sensitive to having their memory space read. A common symptom of this problem is that the hardware adapter (often a communications adapter) does not function properly when DOS shielding is installed. If this is a problem, uncheck the **Check high memory** check box, select the **OK** button to save the settings, and then restart your system to let the new settings take effect.

You can add a local message to the message displayed when viral activity is found by the shield. To do so, modify or create a file named LOCAL.MSG in the same directory as IBM AntiVirus/DOS, and put the text that you want displayed into it. To be displayed properly, the message in this file should have no more than 55 characters in each line and no more than 512 characters total. (You should count each new line past the first line as requiring an additional two characters.)

No change is made to your current DOS sessions. If you want virus shielding in these DOS sessions, first tell IBM AntiVirus/DOS that you want DOS shielded. Then restart your system.

If a virus is found, we strongly recommended that you open IBM AntiVirus/DOS and check your system for viruses as soon as possible.

Additional help is available for:

OK
Cancel

Help for Shield DOS OK

Use the **OK** push button to confirm that you do or do not want DOS shielding to be installed when DOS is started.

No change is made to your current DOS sessions. If you want virus shielding in these DOS sessions, first tell IBM AntiVirus/DOS that you want DOS shielded. Then restart your system.

Help for Shield DOS Cancel

Use the **Cancel** push button to close the Shield DOS pop-up window and return to the previous window. No action is taken.

Help for Settings Not Valid

The advanced options that describe how the system should be checked for viruses contain choices of drives, directories, or files that are not valid. This situation can occur if remote drives were specified and these drives are not currently available to your system, or if a directory or file that was specified no longer exists.

To remove the items that are not valid, select them in the selection box, then select the **Remove** button. When the last item that is not valid is removed the pop-up window closes.

Additional help is available for:

Remove
Cancel
Advanced options

Help for Remove

Select the items that are not valid and that you want to remove from the selection box. Then use the **Remove** push button to remove them and to save the updated settings.

Help for Settings not valid Cancel

Use the **Cancel** push button to close the pop-up window and go to the **Advanced options** pop-up window. Any items that are not valid and that remain are not corrected.

Help for Log window

Logs of your current and previous sessions of IBM AntiVirus/DOS are viewed with a standard browser. You can scroll the text with the scroll bars on the edges of the window. To close the browser, double-click on the System-menu symbol, or select Exit from the Search menu. You can search for text within the file by selecting Find from the Search menu. You can go to the next instance of your search text by selecting Next from the Search menu.

Help for Contacts window

The **Contacts** pop-up window contains information about whom you can contact if you find a virus or if you have questions about the operation of IBM AntiVirus/DOS.

Keys help

The following keys can be used instead of menus to access some of the common functions of IBM AntiVirus/DOS. When two key names are joined by a plus sign (+), use these two keys together. Hold down the first key and press the second key simultaneously.

Ctrl+A	Set up automated checking for viruses
Ctrl+C	View current log of checks for viruses
Ctrl+D	Check diskettes for viruses
Ctrl+F	Product information
Ctrl+G	General help
Ctrl+H	Shield DOS from viruses
Ctrl+I	Help index
Ctrl+L	View cumulative log of automated checks for viruses
Ctrl+O	Contacts
Ctrl+P	View previous log of checks for viruses
Ctrl+S	Check your system for viruses
Ctrl+U	Using help
Ctrl+V	Virus descriptions
F1	Context-sensitive help
F3	Exit IBM AntiVirus/DOS

Authors

IBM AntiVirus Research and development staff:

Bill Arnold
David M. Chess
Vincent J. Cina Jr.
Anni Coden
Alan S. Fleishman
Jeffrey O. Kephart
Charlie Parker
Rhonda Rosenbaum
Alla Segal
Greg Sorkin
Steve R. White

Introduction to computer viruses

This section gives a brief introduction to computer viruses: what they are, how they can spread, and what they can do.

Further information is available on:

What is a computer virus?
How do virus infections start?
How serious is the problem?
Anti-virus programs
IBM AntiVirus Services
For further reading

What is a computer virus?

A computer virus is a program that can "infect" other programs by modifying them to include a (possibly "evolved") copy of itself.

Viruses can spread themselves, without the knowledge or permission of the workstation users, to potentially large numbers of programs on many machines. Viruses can also contain instructions that cause damage or annoyance; the combination of possibly-damaging code with the ability to spread is what makes viruses a considerable concern.

Viruses are not mysterious. They are just computer programs and only do things that programs can do. However, unlike most other programs, they are specifically designed to spread themselves.

Viruses can often spread without any readily visible symptoms. When a virus is started on a workstation, it can run any instructions that its author chooses to include. These instructions can be event-driven effects (for example, triggered after a specific number of executions), time-driven effects (triggered on a specific date, such as Friday the 13th or April 1st), or can occur at random.

Depending on the motives of the virus author, a virus can contain no intentionally harmful or disruptive instructions. Or, it can cause damage simply by replicating itself and taking up scarce resources, such as hard disk space, CPU time, or network connections. Some typical things that some current Personal Computer (PC) viruses do are:

Display a message.
Erase files.
Scramble data on a hard disk.
Cause erratic screen behavior.
Halt the PC.

Many viruses do nothing obvious at all except spread! You cannot rely on strange behavior to find viruses. The most reliable way to find viruses is to use competent anti-virus software as discussed later.

The idea of computer viruses was first developed in its current form in 1983. Since then, people have written many viruses. Viruses are a relatively new problem and require some new approaches to deal with them effectively.

Although it is possible to write a virus for virtually any computer, the viruses that are commonly spreading in the world today are limited to microcomputers. There are no known viruses in circulation that run in native sessions of IBM's OS/2, AIX, VM, MVS or OS/400 operating systems. Any of these operating systems that run PC-DOS programs are capable though, of spreading PC-DOS viruses, including DOS sessions of OS/2 and the DOS Emulation Mode of AIX.

Infected files can be stored almost anywhere. They can be stored as files on servers (such as OS/2 LAN servers, AIX LAN servers, or OS/400 network "folders"). Even when they cannot run on the server machine, an infected file on the server can be run by DOS machines on the network and can spread the infection to them.

How do virus infections start?

The viruses under discussion enter organizations (such as companies and businesses) because an infected diskette or program is brought into that organization. Unlike other security problems, viruses often spread from system to system without anyone's knowledge. Viruses are usually spread within an organization by innocent people going about their normal business activities.

Here is an example. Suppose the organization hires an outside person to come in and perform some work. Part of that person's work involves working on one of the organization's personal computers or microcomputers. The person brings in a few programs to aid in this work, such as a favorite text editor.

Without the person having realized it, the text editor was infected by a virus. By using that editor on one of the organization's machines, the virus spread from the editor to one of the programs stored on the organization's machine, perhaps to a spreadsheet program. The virus has now entered the organization.

Even after the outside person took their personal programs when they left, the virus remained on the machine that it infected in the spreadsheet program. When another employee used that spreadsheet subsequently, the virus spread to another program, such as a directory listing program that the employee kept on the same diskette as the spreadsheet data files. The listing program now is also infected. The infection might spread to other computers to which this diskette disk is taken or, if the employee's personal computer is connected to the organization's network, the employee might send the listing program to another user over the network. In either case, the virus can spread to more users and more machines using diskettes or networks. Each copy of the virus can make multiple copies of itself and can infect any program to which it has access. As a result, the virus can spread widely in the organization.

Each of the infected programs in each of the infected machines can start whatever other instructions the virus author intended. If these instructions are harmful or disruptive, the pervasiveness of the virus causes the harm to be widespread.

How serious is the problem?

Traditional security measures have attempted to limit the number of security incidents to an acceptable level. A single incident of lost files in a year might be an acceptable loss, for instance. Although this is important, it only addresses part of the problem of viruses. Because a single virus could potentially spread throughout an organization, the damage it could cause might be much greater than what could be caused by any individual computer user. The problem is that viruses modify software in an uncontrolled way, which can damage the software. In addition, some viruses actually tamper with data files and can damage the data.

Limiting the number of initial virus infections in an organization is important, but it is often not feasible to prevent them entirely. As a result, it is important to be able to deal with them when they occur.

The **potential** damage is indeed large. By using IBM AntiVirus, and following the advice given here, our experience is that most virus incidents can be managed with little difficulty.

Anti-virus programs

In this section, we discuss the principles and functions of anti-virus programs. It is impossible to completely prevent systems from becoming infected as long as new programs can be introduced on them or their existing programs can be modified. It is also impossible to detect all possible viruses without error. Therefore, it is always possible for systems to become infected. It is important to plan for prevention to the extent possible but equally important to plan for containment and recovery of infections when they do occur.

Further information is available on:

What are anti-virus programs?
Techniques used by anti-virus programs
Techniques used by IBM AntiVirus

What are anti-virus programs?

To understand anti-virus programs, it is useful to understand the basic behavior of known viruses. Generally, all viruses insert copies of themselves in one or more of the following:

Program files (typically stored on diskettes or hard disks).
Boot records (initialization areas on diskettes or hard disks).

Anti-virus programs take advantage of either the general characteristics of all viruses (that they change file or boot records), or characteristics of specific viruses or classes of viruses. The latter kind of program examines the system for something characteristic of either the behavior, or the appearance of specific viruses or classes of viruses. When it finds something with one of these characteristics, it can warn the user, try to prevent the virus from spreading, and so forth.

Techniques used by anti-virus programs

This section discusses some of the common techniques used by anti-virus programs-their advantages and their limitations. It is intended as a technical introduction for people who want to understand how anti-virus programs work.

Further information is available on:

Scanning
Change detection
Heuristic analysis
Verification
Disinfection
Resident and non-resident operation
Automated operation
Prevention and detection
Missing viruses and false alarms

Scanning

When a virus is known and has been analyzed, it is possible to write a program that detects any file or boot record that is infected with that virus. In most cases, the detector can simply look for a pattern of bytes found in the virus but not found in normal programs. Detectors that look for these patterns of bytes are called scanners.

For many viruses, this pattern is a simple, sequential string of fixed bytes. For other viruses, more complicated byte patterns are needed. Care must be taken to ensure that the pattern of bytes is not also found in normal programs, or the detector will report a virus when there is none.

Change detection

Viruses must change files or boot records in order to infect them. A program that notices when files and boot records change can be used to detect viruses even if these viruses were not previously known. But files and boot records change for many normal reasons unrelated to viruses. By itself, change detection is of limited usefulness because it requires users to understand which changes are normal and which changes indicate a virus.

Heuristic analysis

Heuristic analysis attempts to detect viruses by watching for appearance or behavior that is characteristic of some class of known viruses. It can look in files for operations that viruses use but that are seldom used in normal programs. Or it can watch for attempts to write to hard disks or diskettes in unusual ways.

Like change detection, it can potentially detect whole classes of viruses, but care must be taken to ensure that normal programs are not identified as infected.

Verification

The above techniques can indicate that a file or boot record is infected with a virus, but by themselves they cannot be sure nor can they identify with certainty which virus it is. Programs that perform this identification task are called verifiers. Verifiers can be written for known viruses after careful analysis of them.

Disinfection

When a virus is found in a file or boot record, it might be possible to remove it and restore the file or boot record to its original, uninfected state. This process is called disinfection.

Some viruses damage the files or boot records that they infect so that it is not possible to disinfect them successfully. It is also possible for two different viruses to be identified as the same virus by a scanner and for a disinfector to work correctly on one virus but not the other.

Because disinfectors change your programs, they must be very reliable.

Resident and non-resident operation

The techniques discussed above can be used in a variety of ways. One common way for them to be used is in programs that examine everything on your disks, trying to find and eliminate viruses. Another common use is in resident programs in DOS that are always actively monitoring your system for viruses.

Resident programs have the advantage of checking programs for infection every time you run them. Unless they are carefully constructed, they can cause delays in program loading and execution.

Non-resident programs have the advantage of looking for and dealing with viruses on your entire system at one time. They serve as a complementary function to resident programs.

Automated operation

If users have to remember to run an anti-virus program periodically, experience has shown that they will forget, increasing their risk of infecting their systems with a virus and of spreading the virus to other systems.

A better approach is to make sure that the anti-virus program operates automatically. Such programs protect the system without requiring you to take any explicit action. This protection can be accomplished by installing resident anti-virus programs when the system is started and by running non-resident programs, either at startup or periodically at a specified time.

Prevention and detection

Detecting that a virus exists and determining what is infected are important first steps in taking corrective action in a virus incident. Preventing a virus from spreading is important in limiting the size of the infection.

Missing viruses and false alarms

In general, it is impossible to detect all viruses that might ever exist and never make mistakes. Virus detectors will always fail to detect some viruses, incorrectly claim that a normal program is infected, or both.

This failure is not a limitation of current technology. Rather, it can be proven mathematically. Any claim that a program can detect all possible viruses and not make mistakes is untrue.

It is possible, on the other hand, to correctly identify infections from all viruses that we currently know. It is also possible to detect large classes of viruses without making mistakes. By carefully balancing accurate detection with techniques for avoiding false alarms, the risk due to viruses can be drastically reduced.

Techniques used by IBM AntiVirus

This section discusses the techniques used by IBM AntiVirus to provide you with extremely reliable virus protection.

Further information is available on:

Change detection and fuzzy scanning
Heuristic analysis
Verification before disinfection
Thorough examination
Install and forget operation
Advanced false alarm elimination
DOS shielding
Intelligent incident management

Change detection and fuzzy scanning

IBM AntiVirus uses change detection for two purposes. The first purposes is as a starting point for heuristic analysis to detect new viruses, which is discussed in the next section. The second purpose is to make known virus detection faster.

Viruses must change files or boot records in order to infect them. If a file did not have a virus yesterday when we checked it and if we know that the file has not changed, then we know that it does not have a virus today. As it is normally used, IBM AntiVirus only looks in changed and new files for the viruses that it knows about. It is faster to see if a file has changed or is new than it is to examine it for known viruses. This process speeds up the check. (All specified boot records and files are checked for changes and other features, even if they are not examined for known viruses.)

When IBM AntiVirus looks in files and boot records for known viruses, it uses a technique called "fuzzy scanning." This scanning technology used by IBM AntiVirus looks for sequences of bytes that indicate the presence of a virus, as do most scanners. In addition, it recognizes when the sequence of bytes is almost (but not exactly) matched. An inexact match is likely to indicate the presence of a variant of a known virus, and IBM AntiVirus reports the file or boot record as probably infected when it shows you the virus infection report. You will be given the opportunity to remove any such virus.

This technique allows IBM AntiVirus to detect, and correctly identify, a wide range of new virus variants. Without additional measures, this "fuzzy matching" could lead to more false alarms. IBM AntiVirus keeps its identifications highly reliable by advanced false alarm elimination, which is discussed in a subsequent section.

IBM AntiVirus Heuristic analysis

IBM AntiVirus is not limited to detecting viruses that we already know about. It uses heuristic analysis to detect previously unknown viruses as well. It looks for patterns of changes in files, and for features of programs, that are typical of large classes of known DOS viruses. If it finds anything that matches these criteria, IBM AntiVirus will report the files or boot records as "suspicious" when it shows you the virus infection report. You will be given the opportunity to erase/overwrite any such suspicious file.

IBM AntiVirus heuristic analysis has been carefully designed to avoid false alarms. It does not report boot records or files as suspicious just because they have changed. Boot records and files change on computers all the time for reasons unrelated to viruses. It only reports files as suspicious if their pattern of change is typical of virus infections.

Verification before disinfection

When IBM AntiVirus finds what appears to be a known virus, it checks every relevant byte of the virus to determine that it is exactly as expected. This check is very important. If the virus can be verified to be the one expected, then the file or boot record can often be disinfected safely. If the virus turns out to be different, it might have changed the file or boot record in unexpected ways.   Attempting to disinfect it could result in a damaged file or boot record.

IBM AntiVirus does not attempt disinfection if it will result in damaged files or boot records. Instead, it gives you the option of erasing/overwriting the infected files or boot records. In cases where disinfection could result in damaged files, but it might not, IBM AntiVirus records this fact in the log file of your IBM AntiVirus session. You can then examine these programs in more detail and determine whether you should restore them from backups.

Some viruses damage programs that they infect and make it impossible to disinfect them safely. IBM AntiVirus recognizes these cases and deals with them properly. When it disinfects files and boot records, IBM AntiVirus does everything it can to make sure you are not left with malfunctioning programs.

Thorough examination

When you do an initial check for viruses, you might be checking only some of the files or drives on your system. For instance, you might check only program files, because viruses do not typically infect any other files. Checking only program files is how IBM AntiVirus is normally used and is a good way to minimize the time it takes to do an initial check.

If the initial check finds a virus, it is possible there are files you have not yet checked that are also infected. When you do not find all of the infected files and boot records, it is very likely the virus will continue to spread on your system and perhaps spread to other systems as well.

When IBM AntiVirus finds a virus during the initial check, it can then check your entire system thoroughly. It checks all files on all local fixed disks, even if they have not changed, and lets you eliminate any viruses found.

If your system is infected, it is likely that the virus came from a diskette recently or that you have accidentally spread the virus to a diskette. IBM AntiVirus reminds you to check all diskettes that you might have used recently, and lets you eliminate any viruses you find on them. This check is an important step to take to stop the local spread of the virus.

Install and forget operation

IBM AntiVirus is designed to do the correct thing automatically. You do not need to develop a detailed understanding of viruses or anti-virus technology for IBM AntiVirus to protect your system.

Unless you change the default settings for IBM AntiVirus your system will be checked periodically for viruses, and known viruses that attempt to spread in DOS will be detected and stopped. You are notified of any viruses that are found, and are given recommendations about what to do.

Advanced false alarm elimination

Anti-virus programs should both reduce the risk of your system being affected by a virus and avoid bothering you if you do not have a virus. IBM AntiVirus uses a variety of techniques to ensure that known viruses are found and removed reliably and that variants and unknown viruses are likely to be found as well.

IBM has gone to great lengths to eliminate false alarms from IBM AntiVirus. IBM AntiVirus is tested on a collection of several hundred megabytes of normal (uninfected) programs to help ensure that common programs are not identified as infected. However, this is not enough. It is impossible to have every program in the world in this collection so there might be a program somewhere that causes problems.

To help solve this problem, IBM has developed an advanced statistical model to characterize what normal programs look like. All virus search patterns used by IBM AntiVirus are tested against this model and any that have too high a chance of being found in normal programs are rejected, even if they are not found in any of the normal programs in the test collection.

Finally, IBM's internal Personal Computers (PCs) are used as a test population. IBM has over 250,000 PCs. We test IBM AntiVirus on a large number of these PCs before releasing it to help ensure that any problems are found and corrected before you ever see them.

DOS shielding

DOS viruses that infect program files spread when those programs are started under DOS. If you have installed DOS shielding, IBM AntiVirus will warn you when a program that you are running is infected with common, known viruses. In addition, it prevents these viruses from spreading and lets you run the program as if it was not infected at all.

This has two important benefits. First, you can usually run your critical applications even if you have just discovered that they are infected. It is not necessary to shut down your system and deal with the virus immediately (though it is a good idea). Second, you can usually run IBM AntiVirus from your fixed disk, even if the system is infected. It is seldom necessary to shut your system down and restart from a diskette to handle a virus infection. Instead, you can tell IBM AntiVirus to remove the virus and quickly go on with what you were doing. This ability makes it more likely that the infection is taken care of quickly and safely.

To view the list of viruses that IBM AntiVirus knows about, select **Virus descriptions** from the **Help** pull-down on the main window. Then select **List of viruses detected by IBM AntiVirus** from the help screen. Viruses that are prevented by the shield are marked on this list.

Intelligent incident management

IBM AntiVirus is based on IBM's years of experience in handling virus incidents around the world. Dealing with viruses correctly and safely without the proper training can be difficult. We have built our anti-virus expertise right into IBM AntiVirus so that you can protect your systems from viruses without becoming a virus expert.

IBM AntiVirus provides default settings that offer the right protection for most systems. If a virus is found, IBM AntiVirus will lead you through the proper steps to remove the virus from your system.

IBM AntiVirus products and services

IBM AntiVirus products and services are available in several countries around the world. The details of IBM AntiVirus Services differ from country to country; they typically offer:

- Site licenses for IBM AntiVirus/DOS and IBM AntiVirus/2, including regular updates.
- Support for distributing and installing IBM AntiVirus from LAN servers.
- Support for restricting end users from having IBM AntiVirus remove viruses, while permitting anti-virus personnel to do so.
- Site license for the IBM Virus Information Manual, a document that describes known viruses and discusses successful enterprise strategies for limiting their spread.
- Assistance in managing virus incidents.

For more information, please consult the list below. In countries that are not yet listed, please contact your IBM Marketing Representative for more information.

Canada For information on IBM AntiVirus Services, call (416) 946-3786.
Denmark For information on IBM AntiVirus Services, call (+45) 45 93 45 45.
Netherlands For information on IBM AntiVirus Services, call ++31 30 383816.
United Kingdom For information on IBM AntiVirus Services, call Basingstoke (0256) 344558.
United States For single copies of IBM AntiVirus/DOS or IBM AntiVirus/2, call (800) 551-3579. For information on site licensing and IBM AntiVirus Services, call (800) 742-2493.

For further reading

The following recommended reading is for those who want more information about viruses and related topics:

1. Fred Cohen, "Computer Viruses: Theory and Experiment", **Computers and Security,** Vol. 6 (1987) pp. 22-35. This is the first paper that defined viruses in the form that they appear today.
2. **Communications of the ACM,** Vol. 32 No. 6 (June 1989) has several good articles on the Internet Worm incident.
3. Lance J. Hoffman (ed.), **Rogue Programs: Viruses, Worms, and Trojan Horses,** Van Nostrand Reinhold, New York (1990), ISBN 0-442-00454-0. This book is a very good collection of articles spanning many aspects of the virus problem.
4. **Virus Bulletin,** published by Virus Bulletin, Ltd.; 21 The Quadrant; Abingdon Science Park; Abingdon, Oxfordshire OX143YS; England, UK. This monthly newsletter can help technical personnel keep up with the PC virus field.

Virus descriptions

This section contains a list of known DOS viruses that are detected explicitly by this version of IBM AntiVirus/DOS. It also contains descriptions of all of the known DOS viruses that are widespread in the world at the time of this writing. These include all of the viruses that you are likely to encounter in real incidents.

IBM AntiVirus/DOS also detects a large number of viruses that are not in this list. It detects viruses that are similar to the viruses listed here using "fuzzy scanning". It also detects currently unknown viruses using heuristic detection. Please see the Introduction for more information on these techniques.

Further information is available on

Viruses detected by IBM AntiVirus/DOS
Cross-reference of virus names
Descriptions of some known DOS viruses

Viruses detected by IBM AntiVirus/DOS

This section lists the names of known DOS viruses detected by IBM AntiVirus/DOS. Descriptions of the more common of these viruses can be found in the next section.

Computer viruses are called by a variety of names, and there is no universal naming standard. Sometimes, different people refer to the same virus by different names, or to different viruses by the same name. These are the virus names used by IBM AntiVirus/DOS.

All of these viruses can be detected when checking disks and diskettes. Viruses that are similar to these viruses will be detected as well. In many cases, even viruses that are not similar to these will be detected as "suspicious" by IBM AntiVirus/DOS.

An asterisk (*) to the left of a virus name indicates that DOS session shielding will prevent this virus from spreading in DOS sessions. A plus sign (+) to the left of a virus name indicates that it can be verified as identical to IBM's standard sample, and disinfected. In most cases, we have focussed DOS session shielding and disinfection on viruses that are known to be spreading in the world, in order to save space. In some cases, very rare viruses have been added provisionally or for experimental purposes.

```
   !NPO0000-609
   !1019
   _KAMIKAZ
   _150
   AandA.506
   ADA
   Adolf
   Agiplan
   AIDS II
*  Aircop
   Aircopng
   AKUKU
   Alabama
   Albania
   Albania-429
   ALBANIAN-1991
   ALEX_368
   Alexander
   Ambulance
   Ambulance-B
   Andryushka
   Andryushka-3568
   Angarsk
   Angelina
   Animus
   Animus-CooKie
   ANTHRAX
   Anti-D
   AntiPascal-400
   AntiPascal-440
   AntiPascal-480
   AntiPascal-529
   AntiPascal-605
   Anto
   April 1st COM
   April 1st EXE
   Arab
   ARCV4-664
   Argentina
   Armagedon
   Arriba
   Arusiek-817
   Ash
   ASH-743
   Astra-1010
   Astra-976
   AT II 114
   AT II 118
   AT II-122
   AT-132
   ATAS-3215
   ATAS-3233
   Atas-384
   Atas-400
   Athens
   Attention
   AT108
   AT140
   AT144
   AT149
   AUGUST16
*+ Azusa
   Azusa.b
   Backtime
   BAD
   Bad Boy
   BadGuy
   Badsec
   Baobab
   BARCELON
   BARROTES-1310
   Basic
   BB
   BEAST
   BEAST_B
   Bebe
   BEER-2850
   BEER-3164
   Best Wishes
   BESTWISH
   Betaboys
   Beware
   BFD
   Big Joke
   BIOS
   BIRDHOP
   BITADDCT-477
   Black Monday
   Black Peter-1835
   BLACKWIZ
   Blaze
   BLINKER
   BLJEC.3
   BLJEC.4
   BLJEC.5
   BLJEC.6
   BLJEC.7
   BLJEC.8
   BLJEC.9
   BLJEC3B
   BLJEC4B
   BLJEC5B
   BLJEC6B
   BLJEC7B
   BLJEC8B
   BLJEC9B
   BLKWIZ_2
   Blood
   BLOODLUS
 + Bloody!
 + Bloody!-B
   BNB
   BNU
   Bomber
   Boojum
   BOOT437
   BORDER
*+ Bouncing Ball
   Bouncing Ball/286
   Boys
*  Brain
   Brain-Ashar
*  Brain-Shoe
   Brainy
   Brasil
   Breeder
   BRENDA
   BROTHERS
*+ Brunswick
   BRYANSK-673
   Budo
   Bulgarian-123
   Burger-1269
   Burger-405
   Burger-501
   Burger-537
   Burger-541
   Burger-542
   Burger-560
   Burghofer
   BUSH
   BUSTED
   BW970
   BW970B
   Byb-1658
   C_297
   CALC-1939
*+ Campana
*+ Campana-B
```

```
   Cannabis
   Cannabis.b
*+ Cansu
   CAPITALL
   CARA
   Carioca
   Cascade-YAP
   Cascade-1621
   Cascade-1661
   Cascade-1701-D
   Cascade_1701-F
   Cascade_1706
   Casino
   CASTEGGI
   Catman
   CAZ
   CAZ1159
   CB1530
   CCCP-510
   Cerburus-1353
   CFSK-918
   CHAD
   CHCC
   Checksum-100
   Checksum-101
   Checksum-156
   Cheeba_1.1
   Chemist-650
   CHINA-1831
*+ Chinese Fish
   Christmas Violator
   CHV 2.0
   CHV 2.1
   Cinderella
   Civilwar-224
   CLOCK
   Clonewar
   Close
   Cloud
   CLS_853
   CMD-1701
   CMD-549
   Cod
   Code Zero
   Color
   COMMY
   Como Lake
   Companion
   COMX
   Copmpl
   Cops
   Copyright
   Cossiga
   COSTEAU
   CPSU-2535
   CPW-1459
   Cracky
   Crash-1075
   Crazy Eddie
   Crazy Imp
   Crazy Imp-1402
   Creeper-252
   CREEPER-475
   Crew-2480
   CREW_3
   CREW1C-2480
   Criminal
   Crooked
   CSFR1000
   CSL
   CSL-V4
   CSL-V5
   CSSR-528
   CVI-10460
   CVIRUS19
   CVIRUS20
   Cysta-2711
   Cysta-2954
   Cysta-8045
   CZ2986
   D-163
   D_FX
   Dada
   Damage.0
   Damage-b.0
   Danish Tiny-251
   DAPDM_13-709
*+ Dark Avenger
   Dark Avenger family
   Dark Avenger-2100
   Dark End
   DARK_2C-651
   DARTH1
   darth2
   darth3
   darth4
   Data Molester
   DataCrime II
   DataCrime II-B
   DataCrime-1168
   DataCrime-1280
   DATALK2-1043
 + DataLock
   DataLock family
   Datar 1.0
   Datar 2.2
   Dave-1173
   Day 10
   dBASE Destroy
   DBF
   DC_B
   DEADPOOL
   December 24th
   DEICIDE
   Deicide 2
   DEIC2378
   DEIC2543
   DEI2_BRO-693
   Demise
   DEMOL
   DEMON
*  Den Zuk
   Den Zuk 3.c
   DENZUK2
   Destructor
   Devil's Dance-941
   Dewdz
   Diamond family
   Digger
   Dima
   DINAMO
*  DIR II
   DIR II-H
   DIRVIR
   DIR760
*  Disk Killer
   Diskspoiler
   Dismember-288
   DM-310
   DM-400
   DM_400
   DM400
   Do Nothing
   Do Nothing 2
   Doom 2
   Doom 2-B
   DOOM-1B
   DOS_625
   DOShunt-483
   Dot Killer
   Dr. Qumak II
   Drop
   Dudley-1153
   DUPACEL-8192
   Dutch
   Dutch Tiny-99
   Ear
   Eastern D-1600
   Eastern Digital
   ED-779
   Eddie 2-B
   Eddie 2-C
   Eddie-651
*  EDV
   Eight Tunes-1971
   Einstein
   Elenam
 + Eliza
   ELM-718
   ELOI-1273
   EMF
   Emmie
   encrboot
   End of-783
   Enemy
   Enigma
   Enigma 2
   Enola
   EST_1716
   ETC
   EUPM
   Europe'92
 + Even Beeper-B
   Evil Empire
   Evil Empire-B
   Evil Empire-C
   Evil Empire-C2
 + Evil Empire-C3
   Evil Empire-D
   EXE_222
   EXEBUG
   EXEBUG-H
   EXEBUG-2
   EXEBUG-3
   Exterminator
   F-Soft 458
   F-WORD
   F-709
   FACE
   Fake-VirX
   Falling boot.c
   Falling Letters Boot
   Fame-896
   Father
   FCB
   Feist
   Fellowship
   Fichv EXE 1.0
   Filedate 11-537
   Filler
   Fingers
   Finnish-357
   Fish 6
   FISH-1100
   FISH-2420.DMC
   FLASH
   Flash-Gyorgy
*+ Flip-2153
   Flip-2153-B
   Flip-2153-C
   Flip-2153-D
*+ Flip-2153B
*+ Flip-2343
   FLOWER
   FMC-775
   FORGER
*+ FORM
   FRAJER-649
   Freddy-1870
   Freew-692
   Freeze
   Friday the 13th COM
   FRIDAY13
   Friends
   FRI13_QF
   FRODO_D-4096
   FRODOSFT-458
   Frog's Alley
   FRUSTRAT-632
   Fumble-867
   FUMBLE3
   Funeral-921
   GEEK-450
   GENB1
   Gergana
   Gergana-222
   Gergana-300
   Gergana-450
   GERG512
   Ghost
   GHOST_0
   GIPSY-304
   Gliss
   Goodbye
   GORLOVKA
   GOSIA
   Got_You
   Gotcha-D
   Gotcha-E
   GOTCHA_A
   GOTCHA_B
   GOTCHA_C
*+ Grain of Sand
   Grapje
   Greemlin-0
   Grune-1241
   GULLION
   Guppy
   GYRO
   Gyro
   HACKER-3 (HORSE3)
   HACKER-5
   HACKER_1
   HACKER_2
   HACKER_7
   HAF_1187
   HAFEN_E
   Hafenstrasse
*+ Haifa
*+ Haifa-Motzkin
 + Halloechen
   Halloween
   HANGER
   HAPPY
   Happy
```

Happy Day
Happy Monday A
Happy Monday B
Happy Monday C
HARAKIRI
Hary Anto
Hastings
Headache
Hell-1182
Helloween-1376
Hero
Hero-394
Hey You
HH&H
HI_460
Hide and Seek
Highlander-477
Hitchcock
HOCH-950
Horror
Horror-1112
Horror-1137
Horse (1) Family
Horse (2) Family
Horse Boot
Horse 4
HR
Hungarian-473
Hungarian-482
Hybryd
HYDRA
HYDRA_1
HYDRA_2
HYDRA_3
HYDRA_4
HYDRA_5
HYDRA_6
HYDRA_7
HYDRA_8
Hymn
Ice-9
Iceland II
Ieronim
Ieronim-1581
Ieronim-512
Ieronim-560
Ieronim-600
Illness
INCOM
Infector
Infinity
INTERC
Intruder
INT13
Int86
INVOL
Ionkin

```
   IPA
   IPER-1062
   Iron Maiden
   IRUS
   Itavir
   Itti-Malmsey
   Itti-191
   Itti-99
   Jabberwocky
   JABBER1
   Japanese Christmas
   Japanese Cookie
   JD-158
   Jeff
   Jer-Count
   Jer-Zipeater
   JERCZEHA
   Jerry-2074
   Jerusalem-IRA
   Jerusalem-Mummy
   Jerusalem-1767
   Jerusalem-2187
   JERU1663
   Jihuu
   jktk
   Jocker
   JOJO
   Joker-01
   JOKR1371
*+ Joshi
 + Joshi-B
*+ Joshi-00
   July 13th
   June 16th ("Pretoria")
   Junior-234
   JUSTICE
   Kalah
   Kalah-499
   Kamikaze
   KAMPANAB
   KARIN
   Kemerovo
   Kemerovo-B
   Kennedy-163
   Kennedy-333
   Keyboard Bug-1596
   Keyboard_Bug
   Keypr-1266
*+ KeyPress
   Keypress-Chaos
   Keypress-1479
   Keypress-1774
   Kiev-2049
   Kiev-483
   Kiev-483A
   Kiev-493
   killer
   kilroy
   Kinnison
   Kiss
   KIT
   KIWI-550
   Klaeren
   KLAW-752
   KLF_356
   KODE4-399
   KODE4V1
   KO408
   KRIVMOUS
   Kthulhu-512
   KUKU-448
   Kylie
*  Lao Doung
   Larry
   Larry-491
   LAZY
   LBC
   Leech
*  Lehigh I
   LEPRMUTA
   LEPRMUTB
   Leprosy
   Leprosy-B
   Leprosy-Busted
   Leprosy-B2
   Leprosy-C2
   Leprosy-D
   Leprosy-Viper
   Leprosy-Wake
   LEPROSYC
   LEPROSYF
   Lesson II-358
   Lesson 1
   Lesson 2-B
   Lesson 2-360
   leszop
   leszop2
 + Liberty
   Liberty Boot
   Liberty-SSSSS
   LIBERTY2
   Lippi-286
   Little Brother
   Little Brother-300
   Little Brother-307
   Little Brother-321
   Little Brother-349
   Little Girl
   Little Pieces
   LM-305
   LNCSPWI1
   LNCSPWI2
   LOG
 + LOL
```

```
   LORD_933
   LOS-693
   love
   LoveChild
   Lovechild-B3
 + Lowercase
   Lozinsky
   Lozinsky-1018
   LPTOFF
   Luca-309
   LYC_1888
   Lyceum-1788
   Lyceum-1832
   Lyceum-1975
   LYTHYUM-502
   LZR
   Macedonia
   MADE
   Maffy-323
   Maffy-478
   Maffy-491
   Magnit-2560C
   Magnitogorsk
   MAGN2048
   Malaga
   malaga
   MALAISE
   MALIG-575
   MALIG-630
   MANNEQUI-778
   MannequinB-778
   MANUEL-957
   Marauder
   Marauder-B
   Marauder-560
   Mardi Bros
   Matura
   MAUS1888
   Mayak-2339
   MCWHALE
   MEDITAT-299
   Meditation
   MEGAF
   MERDE_6-354
   META1103
   MEXICAN
   MGN-3000
   MGN2048B.DMC
   MGTU
   MG1
   MG3
*+ Michelangelo
   Micro-128
*  Microbe
   MICROPOX
   MIKOLA_B
   MIKRO45A
```

```
  MIKY
  Milena
  MILOUS
  MINI-45
  Minimal-30
  Minimal-30-B
  Minimal-46
  MINIMAX
  Ministry
  MIN38
  MIN39
  MIN44
  Mirror
  Mithrandir
  MIX1
  MIX1-B
  MIX2
  Moctezuma
  Monkey-1
  Monkey-2
  Mono-1063
  MORE-718
  Mosquito
  MPHTI
  MPH2
  MPS 1.1
  MPS 3.1
  MPS 3.2
  MPS-OPC
  MR-253
  MrVir-508
  MS_748
  Mshark
  Mshark-889
  MSHARKN-378
  MSJ
  MSK
  MSTU-531
  MSTU-551
  MSTU-554
  MtE family
  MtE(nul) family
  MUBARK
  Mud
  mugshot
  Mule
  Multiface
  Mummy 1.2
+ MUMMY-21
  Munich
  MURGAS
  Murphy 1
  Murphy 2
  MusicBug
  MX_335
  M32
  M34
```

```
   M40
   Nazgul
   neardark
   NECRO_SH-1200
   New Badguy
   New Sunday
   New Zealand (1)
   NEW_CASC
   NG-914
   Nichols.a
   Nichols.Scythe
   Nina
   NINECOMP-705
   Nines Comp-706
   Nines Comp-776
   NINJA-1616
   NJH-LBC-2
   NKOTB
   NMBR1E
   No Frills-843
   Nobock
   NoInt
*+ Noint
*  Nomenklatura
   NOT-586
   Nov 17th-880
   NOV-7
   NOV11
 + NOV17
   NOV17-584
   NOV17-706
   Nov17-800
   NOV17B
   NOV30
   NPOX11
   NPOX21-1686
   NUKE
   NUKPOX20-1800
   Number 1
   NUMBER1
   NV71
   Nygus
   oak
   ogre2
*  Ohio
   Ohio0
 + Omega
   Ontario
   ONTAR730
   Orion-262
   Orion-365
*  OROPAX
   OTTO-415
   OTTO5-640
   Outland
   OVER4870
   OW-37
```

```
    OW-64
    OXANA-1670
    P_3072_B-3157
  + PADDED
    PANDAFLU
    Parasite
    Parasite 2
    Parasite_2b
    Paris
    Parity
    Parity boot
    PASCAL
    PASSWORD-1271
    Path
    Pathhunt
    PC Bandit
    PC Byte Bandit
    PC Byte Bandit-1658
    PC Byte Bandit-1679
    PC Byte Bandit-1722
    PC-Flu
    PC-FLU 2
    PCV
    PEACH
    PEBBLE
    Pentagon
    PENZA
    Penza-1210
    Perfume-731
 *  Perfume-765
    PERRY2
    PETERBRG
    PHALCON
    Phalcon-899
    Phantom
    Phoenix-Evil
    Phoenix-Phoenix
    Phoenix-Proud
    Phoenix-Trojan
    Phoenix-1226
    Pick-843
    Pif-paf
    Pipi
    PIRATE
    PISELLO
    PITCH-593
    Piter
    Piter-B
    PIX_345
    Pixel-Rosen
    Pixel-257
    Pixel-275
    Pixel-277
    Pixel-283
    Pixel-295
    Pixel-299
    Pixel-345
```

```
   Pixel-740
   Pixel-779
   Pixel-837
   Pixel-847
   Pixel-850
   Pixel-852
   Pixel-854
   Pixel-892
   Pixel-897
   Pixel-899
   Pixel-899B
   Pixel-905
   PIXEL877
   PIXIE
   Plague
   PLAICE
   Plaice
   Plastique (2)
*+ Plastique 4.51
   Plastique 4.51-B
   Plastique 5.21
*  Plastique-Danube
*  Plastique-Invader
*  Plastique-2576
*+ Plastique-2900
   Plastique-3088
   Play Tetris
   Plovdiv
   Plovdiv 1.3
   Plovdiv 1.3B
   PLOV13B
   Plutto
   Poem
   Pojer
   Pojer-1935
   POLEDNE-1666
   POLIMER
   Polish Color
   Polish Minimal-45
   Polish-217
   Poss-A
   Poss-B
   POSSESS2
   POSS107
   PRAGJOKR
   PRE_REL-381
   Pregnant
   Press
   Prime
   PRINTMON-853
   Prob-734
   PROB_854
   Problem-856
   Problem-863
   Protect-1157
   Protect-1355
   Protecto
   PROTO_T-695
*+ PrtSc
   Prudents-1210
   PS!KO_C-1459
   PSQR-1720
   PSYCHO
   QMU-1513
   QRry
   Quake
   QUAKE_O
   QUIET
*+ Quox
   Rage
   Rat
   RAT-615
   RATTLE-615
   Raubkopi
   RCE1049
   RC492
   Reboot Patcher
   Reboot-715
   Red Diav-662
   REKLAMA-2723
   REKLAMOW-2723
   RMIT
   RNA 2
   RNA_(1)
   Rock Steady
   Russian Mirror
   RUST
   Ryazan
   SA_623
   SAD
   Sadam
   SADIST
   saigon
   Saratoga 1
   Saratoga 2
   SATAN-512
   Saturday 14th ("Durban")
   SBC
   Scion
   Scream family
   Scream-family
 + Scream-2b
 + Scream-696
   SCREAMER
   Screamer_II
   Scribble
   SCROLL
   SeaCat
   SECRETS
   SELF_457
   SELF_550
   Semtex
   SEMTEXB
   SENECA2
   SENT_BC
   Sentinel
   SENTINEL5
   SENTINL1
   SENTINL1-4636
   SENTINL2
   SENTINL3
   Seventh Son-284
   Seventh Son-350
   SH-2294
   Shadowbyte
   Shadowbyte-2
   Shake
   SHAKER
   SHHS
   SHHS-B
   Shifter
 + Shirley
   SICKCOOK
   Signs
   Silence
   Silly-117
   Silly-131
   Silver Dollar
   SILVER3B
   SIMPLE-424
   Simulate
   SINEP-644
   SIS_2630
   Siskin-1017
   Siskin-948
   Sistor-1000
   Sistor-2225
   Sistor-2380
   SK-1004
   SK-992
   SKEW_469
   SKISM808
   SK1147
   SLOV_1B
   SLOV2
   SLOV200
   Slow 2
*+ Slow-1721
   Slow-2131 ("Scott's Valley")
   SMAL-104
   SMAL-110
   SMALARCV-236
   SMALL-124
   Small-127B
   Small-129
   Small-130
   Small-132B
   Small-157
   SMALL-178
   Small-185
   Small-187
   Small-409
   SMALLEXE-349
   Smallv-115
   Smiley Worm Boot
   Socha
*  Solano
   Something
   South African 408
   SOV_1205
   Sov1
   Sov2
   Spanish Telecom 2
   Spanz
   Sparse
   SPOOK
   Spyer
   SQUAWK-852
   Squeaker
   Squisher
   STAF
   Stahlplatte
   STANCO
   Stardot family
   Stardot-600
   StarDot-789
*+ Stardot-789
   StarDot-801
 + Stardot-801
   stelboo
   Sticky
   STIGMATA
   Stink
   STINKFOT
   STINK2
   STINK2D
*+ Stoned
   Stoned 2
   Stoned-Alberta
*+ Stoned-C
   Stoned-Hidos
   Stoned-ZAPPED
   stoned8
   STONE90
   stonheng
   STORM-1153
   Striker
   ST2560
   Suicidal
   Suicide
   SUM_1569
*+ Sunday
*  Sunday 2
   Suomi
   Suriv 1-XUXA
   Suriv 3.00
   Surrender-513
   SVC
   SVC 3.1
   SVC 4.0
*  SVC 5.0
   SVC 5.0 B
   SVC 6.0
   SVC-4B
   Sverdlov
   SVIR
   SVS
   Swedish Disaster
   Swiss-143
   Sylvia
*  SYSLOCK
   TABULERO
   TACK
   TACK-B
   TACK-N
   Taiwan
   Taiwan 2
   Taiwan-C
   Talentless Jerk
   Tankard 3.01-556
   Taunt
   Telecom-3700
   Telecom-3784
   Ten Past Three
*+ Tequila
   TERMINAT
   Terminator-1501
   Terminator-918
   TERROR
   Testvirus B
   TETRIS-552
   TH-IP
   THEFAST
   THIMBLE
   Thursday the 12th
   TIC
   TIC_B
   Timemark1
   Timemark2
   TIMEMRK1
   TIMEMRK2
   Timeslice-2330
   Timid-303
   Timid-305
   Timid-306
   TIMOR
   Tiny DI-110
   Tiny Hunter
   Tiny-Mutant
   Tiny-123
   Tiny-127
   Tiny-132
   Tiny-134
   Tiny-138
   Tiny-143
   Tiny-145
   Tiny-154
   Tiny-156
   Tiny-158
   Tiny-159
   Tiny-160
   Tiny-167
   Tiny-198
   Tiny-212
   Tiny-310
   Tiny_DI-101
   Tiny_DI-108
   Tiny_DI-94
   TINY128
   Tired
   TiredBoot
   TISO
   TJack
   TMTMID-441
   TNAME-1086
   TNKRD20-493
   Tokyo
   Tolbuhin
   Tony
   Tony-203
   TONY203
   TOPO
 + Topo
   TOPSY900
   TPWORM
   TP06VIR
*+ TP16VIR
   TP23VIR
   TP24VIR
   TP25VIR
   TP33VIR
   TP34VIR
   TP41VIR
   TP42VIR
 + TP45VIR
   TP46VIR
   Traceback-2930
   Traceback-3029
   Traceback-3066
 + Traveller
   TREE
   Tremor
   Trivial-Banana
   Trivial-30D
   Trivial-31
   Trivial-31B
   Trivial-35
   Trivial-45B
   Trivia1-42
   TRJC_982
 + Troi
   Troi II
   TSOFT-547
   TSOFT-598
   TU-482
   Tula-1480
   Tula-419
   Tula-593
   Tula-635
   TUM-1242
   Tumen
   TUMEN05
   TUMEN1_2
   Turbo-Kukac
   Turbo-448
   TVER-308
   Twelve Tricks Trojan
   Twin
   Twin-351
*+ Typo Boot
   UFA-1201
   Ungame
   URFYDUS
   URUK
   URUK-300
   URUK-361
   URUK-427
   USSR-1594
   USSR-311
   USSR-707
   USSR-830
   UX142
   V_160
   V_176
   V_195
   V_388
   V_550
   V_821
*+ VACSINA
   VACSINA-loader
   VACS44B
*  VBASIC
*+ VBASIC-B
   VCL_YD2B-822
   VCOMM2
   VCS 1.0
   VCS-Post
   VDV853
   Vengeance
   Vengence-A
   Vengence-B
   Vengence-C
   Vengence-D
   Vengence-E
   Vengence-F
   VFSI
   VHP-348
   VHP-353
   VHP-361
   VHP-367
   VHP-435
   VHP-623
   VHP-627
   VI_NEWGN-1054
   Victor
   Vienna Dr.Q
   Vienna family
   Vienna-Choinka
   Vienna-Ghost
   Vienna-Ira
   Vienna-Lisbon
   Vienna-Mob_1A
   Vienna-Monxla
   Vienna-opt
   Vienna-Twer
   Vienna-Viola
   Vienna-Viola B4
   Vienna-1828
   Vienna-535
   Vienna-618
   Vienna-643.DMC
   Vienna-644
   Vienna-644B
 + Vienna-645
   Vienna-646
*+ Vienna-648
   Vienna-656
   Vienna-730
 + Vienna-733
   Vienna-757
   Vienna-776
   Vienna-833
   Vienna-849
   VIENNA_E-648
   VIEN849
   Vindicator
   VIOL_C-821
   Violator C
   Violator-Arf.2
   Violator-B3
   Violator-D
   VIOLB
   Violetta
   Violetta-1024
   VIOOCT31
   VIPERIZE
   Virdem
   Virdem 2
   Virdem.Disktrash
   VIRDEM2
   VIRI
   Virus 9
   VIRUS-90
   VIRUS651
   Vivaldi
   VJABBER
```

```
  VOLG_A
  VOLG_B
  VOLG_CDEF
  VOLG_G
  VOLG_H
  VOLG_I
  Voronezh
  Voronezh-370
  Vote
  VP
  Vriest
  VVF 3.4
  V1024
  V1028
  V1385
  V1463
  V150
  V178
  V1876
  V1920
  V2P6
  V200
  V2000
  V203
  V2144
  V217.a
  V226
  V276R
  V344
  V358R
  V377
  V392R
  V439
  V472
  V483
  V512
  V512-B
  V512-C
  V512-D
+ V512-E
  V516
  V711.2
  V789
  V800
  V84
  V905
  V948
  WABIKCOM-547
  Walker
  Warrior
  Washburn-Casper
  Washburn-V2P2
  Washburn-1260
  Water
  We're_Here
  WHALE
  Whale-B
```

```
   Whirl.a
   whirl2
   Why Windows
   Wildy-354
   WIRUS
   Wisconsin
   WITCODE
   WIZ_3_0-268
   Wolfman
   Wonder
   WONDER2
   Words-1069
   Words-1085
   WWT_01
   WWT_01-67
   WWT_02
   W13-A
   W13-B
   W13-REQ
   X_1
   Xabaras
   XA1
   XFUNGUS
   XPEH
   XPEH-3840
   XPEH-4752
   XPEH-5648
   XPEH-5808
   XPEH-5856
   XPEH_2
   XPEH_3
   XPEH5840
   XUXA945
   YAFO family
   Yafo_2b
   YAFRI13
*  Yale
   Yale.b
   Yan-2505
   YAN_1256
   YAN_1905
   yanboot
*+ Yankee Doodle-2772
*+ Yankee Doodle-2885
   Yankee-Login
   Yankee-1150
   Yankee-1202
   Yankee-1624
   Yankee-1961
   YANKLOGX
   YANK2980
   Yaunch
   Year-6545
   YEKE-1076
   YEKE-1076 family
   YEKE-1204
   YEKE-2425
   YEKE-2425 family
   YOU_FUTH-968
   Youth
   Yukon
   Zero Hunt
   Zero Hunt-B
   Zherkov-1882
   Zherkov-1915
   Zherkov-2968
   Zherkov-2970
   ZHER1915
   Ziuck-1279
   ZK-900
   ZZ
   1024PSCR
   1028
   1067
   1077
 + 1244
   1253
   1355
*  1381
   1392
   1536
*+ 1575
   1590
   1600
   1689
*+ 1701
   1701 family
   1701-Formiche
   1701-Jojo
*+ 1701-Nodate
   1701-S
   1701-Stamm
*+ 1704
   1704-B
   1704-C
   1704-Format
*  1704-Y
   1759
*+ 1813
*  1813-ANARKIA
 + 1813-Captrip
   1813-Carfield
   1813-Clipper
*  1813-Discom
 + 1813-Frere
   1813-GP1
   1813-Groen Links
   1813-not-13
   1813-Puerto
*  1813-Swiss
   1813-Westwood
*+ 1813-00
   1813-1361
   1813-1605
   1840X
*  1963
*  1963-B
   1992
   1992-B
   1993
   2062
   2086
   2560
   2623
   286-PLUS
   302
   337
   3445
   382
   403
*+ 4096
   417
   453
   5lo.2
   512-related
   534B
   534C
   534D
   534E
   534M1-679
 + 555
*+ 555-B
   5792
   600
   637
   664
   696
   7SON2
   757
   765
   777 Revenge
   800
   864
   907
   9800:0000
```

Cross-reference of virus names

Computer viruses are called by a variety of names. Sometimes, different people refer to the same virus by different names, or to different viruses by the same name. This table translates some of the more common names into the name used by IBM AntiVirus/DOS. Since these names are used differently by different people, the entries in this table may not reflect every use of these names by others. Sometimes different people use the same name, but it differs in capitalization (for example, ANTHRAX and Anthrax). In these cases, this table only includes an entry for IBM AntiVirus. capitalization.

NICKNAME	NAME USED BY IBM ANTIVIRUS
Agiplan	Agiplan
AIDS	Taunt
AIDS 2	Companion
Aircop	Aircop
AKUKU	AKUKU
A kuku	AKUKU
Alabama	Alabama
Alameda	Yale
Alexander	Alexander
Ambulance	Ambulance
Ambulance Car	Ambulance
AMOEBA	1392
Amoeba 1392	1392
Amstrad	Pixel-847
ANARKIA	1813-ANARKIA
Andryushka	Andryushka
Andryushka-3568	Andryushka-3568
Animus	Animus
Animus.CooKie	Animus.CooKie
ANTHRAX	ANTHRAX
AntiCad	1253
AntiCad 1	Plastique-2900
AntiCad 2	Plastique-Danube
AntiCad 4.Danube	Plastique-Danube
AntiCad 4.Mozart	Plastique-Invader
AntiCad 5	Plastique-2576
Anticad 3.a	Plastique 4.51
Anticad 3.b	Plastique 4.51-b
Anticad 1.a	Plastique 5.21
Anti-CTNE	Campana
Anti-Pascal II	AntiPascal-480
AntiPascal-400	AntiPascal-400
AntiPascal-440	AntiPascal-440
AntiPascal-480	AntiPascal-480
AntiPascal-529	AntiPascal-529
AntiPascal-605	AntiPascal-605
Anti-Telephonica	Campana
April 1st	April 1st COM, April 1st EXE, Suriv 1.01
April 1st COM	April 1st COM
April 1st EXE	April 1st EXE
Arab	Arab
Arab Star	1813

Armagedon	Armagedon
Armagedon the First	Armagedon
Armagedon the GREEK	Armagedon
Ashar	Brain-Ashar
Austrian	Vienna-648
Austrian 2	1701, 1704
Autocad 2	Plastique-2900
Autumn	1701, 1704
Autumn Leaves	1701, 1704
Azusa	Azusa
BASIC	VBASIC
Bejing	Bloody!, Bloody!-B
Best Wish	555B
Better World	Fellowship
BFD	BFD
Black Avenger	Dark Avenger
Black Friday	1813
Black Hole	1813
Black Monday	Black Monday
Black Window	1813
Blackjack	1704B
Blood	Blood
Bloody	Bloody!
Bloody!	Bloody!
Bloody!-B	Bloody!-B
Bloomington	Noint
Bob Ross	Cloud
Bomber	Bomber
Bouncing Ball	Bouncing Ball
Bouncing Ball/286	Bouncing Ball/286
Bouncing Dot	Bouncing Ball
Brain	Brain
Brain-Ashar	Brain-Ashar
Brain-Shoe	Brain-Shoe
Brunswick	Brunswick
Bupt	Traveller
Burger-405	Burger-405
Burger-501	Burger-501
Burger-537	Burger-537
Burger-541	Burger-541
Burger-542	Burger-542
Burger-560	Burger-560
Campana	Campana
Campana-B	Campana-B
Cansu	Cansu
Captain Trips	1813-Swiss or 1813-Captrip
CARA	CARA
Carioca	Carioca
Cascade	1701, 1704
Cascade-B	1704-B
Casino	Casino
Casper	Washburn-1260, Washburn-V2P2 or Washburn-Casper
Chameleon	Washburn-1260
Chinese Fish	Chinese Fish
Choinka	Vienna-Choinka
Christmas in Japan	Japanese Christmas
CHV 2.0	CHV 2.0

CHV 2.1	CHV 2.1
Cinderella	Cinderella
Cloud	Cloud
Columbus Day	DataCrime-1280, DataCrime-1168, DataCrime II, DataCrime II B
COM	Friday the 13th COM
Commander Bomber	Bomber
Como Lake	Como Lake
Companion	Companion
Computer Ogre	Disk Killer
Cookie-7360	Animus
Cookie-7392	Animus-CooKie
Crash-1075	Crash-1075
Crazy Eddie	Crazy Eddie
Crew-2480	Crew-2480
Criminal	Criminal
CSSR	CSSR-528
CSSR-528	CSSR-528
Cursey	EDV
Danish tiny(163)	Kennedy-163
Danish tiny(Kennedy)	Kennedy-333
DarkAvenger	Dark Avenger
Dark Avenger	Dark Avenger
Dark Avenger 2	Eddie-651
Dark Avenger II	V2000
Dark Avenger III	V1024
Dark Avenger-2100	Dark Avenger-2100
DataCrime	DataCrime-1280, DataCrime-1168
DataCrime B	DataCrime-1168
DataCrime II	DataCrime II
DataCrime II B	DataCrime II-B
DataCrime II b	DataCrime II-B
DataCrime II-B	DataCrime II-B
DataCrime-1168	DataCrime-1168
DataCrime-1280	DataCrime-1280
DataCrime-2	DataCrime II
DataLock	DataLock
Datar 1.0	Datar 1.0
Datar 2.2	Datar 2.2
DataRape 2.2	Datar 2.2
DBASE	DBF
DBase	DBF
DBF	DBF
Dead Kennedy	Kennedy-333
Dead Kennedys	Kennedy-333
Death to Pascal	Wisconsin
December 24th	December 24th
Dedicated	MtE family
DEICIDE	DEICIDE
Demise	Demise
DEMOL	DEMOL
Den Zuk	Den Zuk
DENZUKO	Den Zuk
Devil	Devil's Dance-941
Devil's Dance	Devil's Dance-941
Devil's Dance-941	Devil's Dance-941
Diamond	V1024

Diana	Dark Avenger
DIR 2	DIR II
DIR II	DIR II
DIR II-H	DIR II-H
DIRVIR	DIRVIR
Discom	Discom
Disk Crunching	Icelandic II, Saratoga 1, Saratoga 2, December 24th
Disk Killer	Disk Killer
Disk Ogre	Disk Killer
Do Nothing	Do-Nothing, Do-Nothing 2
Do Nothing 2	Do-Nothing 2
Donald Duck	Stoned 2
Doom 2	Doom 2
Doodle 39	Yankee Doodle-2772
Doodle 44	Yankee Doodle-2885
DOS-62	Vienna-648
DOS-68	Vienna-648
Dudley-1153	Dudley-1153
Durban	Saturday 14th
Dutch	Dutch
Dutch-1039	GRAPJE
Dyslexia	Solano
Ear	Ear
EB 21	PrtSc
Eddie	Dark Avenger
Eddie 2	Eddie-651
Eddie 3	Eddie-651
Eddie-651	Eddie-651
EDV	EDV
Eight Tunes	Eight Tunes-1971
Eight Tunes-1971	Eight Tunes-1971
Einstein	Einstein
Eliza	Eliza
European Fish Viruses	Fish 6
EUPM	EUPM
Even Beeper-B	Even Beeper-B
Evil	Phoenix-Evil
Evil Empire	Evil Empire
Evil Empire-B	Evil Empire-B
Evil Empire-C	Evil Empire-C
Evil Empire-C	Evil Empire-C2
Evil Empire-C3	Evil Empire-C3
Evil Empire-D	Evil Empire-D
Fall	1701, 1704
Falling Letters Boot	Falling Letters Boot
Falling Tears	1701, 1704
Father Christmas	Vienna-Choinka
Fear	MtE family
Fellow	Fellowship
Fellowship	Fellowship
FILLER	FILLER
Fingers	Fingers
First Austrian	Vienna-648
Fish	Fish 6
Fish 6	Fish 6
FLASH	FLASH

Flip	Flip-2343, Flip-2153
Flip-2153	Flip-2153
Flip-2153B	Flip-2153B
Flip-2153-C	Flip-2153-C
Flip-2153-D	Flip-2153-D
Flip-2343	Flip-2343
FORM	FORM
Form Boot	FORM
FORM-Virus	FORM
France	ZK-900
Friday 13th	Friday the 13th COM, 1813
Friday the 13th	Friday the 13th COM
Friday the 13th COM	Friday the 13th COM
Frodo	4096
Fu Manchu	2086
Fu Manchu - Version A	2086
Fumble	Fumble-867
Fumble-867	Fumble-867
Ghost	Vienna-Ghost
Ghost Boot	Vienna-Ghost
Ghost COM	Vienna-Ghost
Ghost Version of DOS 62	Vienna-Ghost
Ghostballs	Vienna-Ghost
Grain of Sand	Grain of Sand
GRAPJE	Grapje
GREEK	Armagedon
Green Caterpillar	1575
Groove	MtE family
Guppy	Guppy
Hacker	Ohio
Haifa	Haifa
Halloechen	Halloechen
Happy Birthday Joshi	Joshi
Happy Day	Happy Day
Hate	Klaeren
Hawaii	Stoned
Hebrew University	1813
Hello (1A)	Halloechen
Hemp	Stoned
Herbst	1701, 1704
Holland	Sylvia
Holland Girl	Sylvia
Holo	Telecom-3784
ibm	Lowercase
Iceland	Iceland II, Saratoga 1, Saratoga 2, December 24th
Iceland I	Saratoga 2
Iceland II	Iceland II
Icelandic	Iceland II, Saratoga 1, Saratoga 2, December 24th
Icelandic II	Iceland II
Icelandic III	December 24th
Icelandic-3	December 24th
IDF	4096
India	PrtSc
INT13	INT13
Internal	1381

Invader	Plastique-Invader
INVOL	INVOL
Ira	Vienna-Ira
Irish	Grain of Sand
Israeli	1813
Israeli Boot	Falling Letters Boot
Israeli Defense Forces	4096
Italian	Bouncing Ball
Itavir	Itavir
Japan	Japanese Christmas
Japanese Christmas	Japanese Christmas
Japanese-Xmas	Japanese Christmas
Jeff	Jeff
Jerry-2074	
Jerry-2074	
Jeru-Discom	1813-Discom
Jeru.Swiss	1813-Swiss
Jeru-Sunday	Sunday
Jeru-Sunday	Sunday 2
Jerusalem	1813
Jerusalem Strain B	1813, 1813-ANARKIA, 1813-not-13, 1813-Swiss
Jerusalem-B	1813
Jerusalem-E	Suriv 3.00
Jerusalem-Milky	MIKY
Jerusalem.Not13	1813-not-13
Joe's Demise	Demise
JOJO	1701-Jojo
Joshi	Joshi
Joshi-B	Joshi-B
Joshi-00	Joshi-00
July 13th	July 13th
June 16th	June 16th
June-the-16th	June 16th
JUNE16	June 16th
JV	1813
Kamikaze	Kamikaze
Kemerovo	Kemerovo
Kennedy	Kennedy-333
Kennedy-163	Kennedy-163
Kennedy-333	Kennedy-333
KeyPress	KeyPress
KeyPress-1479	KeyPress-1479
KeyPress-Chaos	KeyPress-Chaos
KHETAPUNK	1392
Klaeren	Klaeren
Korea	LBC
Kukac-2	Turbo-Kukac
Label	INT13
LastDirSect	Noint
LBC	LBC
LBC Boot	LBC
Leech	Leech
Lehigh	Lehigh I
Lehigh I	Lehigh I
Leprosy	Leprosy
Leprosy 1.00	Leprosy
Leprosy-B	Leprosy-B

Liberty	Liberty
Lisbon	Vienna-Lisbon
Little	MtE family
Little Brother-349	Little Brother-349
Live After Death	V800
Live/Death	V800
LOL	LOL
Lowercase	Lowercase
LZR	LZR
MACROSOFT	SYSLOCK
Maltese Amoeba	Grain of Sand
Many fingers	Fingers
Marauder	Marauder
Marauder-B	Marauder-B
Mardi Bros	Mardi Bros
Marijuana	Stoned
Marti Brothers	Mardi Bros
Mendoza	1813
Merritt	Yale
Mexican	Devil's Dance-941
MG1	MG1
MG3	MG3
MGTU	MGTU
Miami	Friday the 13th COM
Michelangelo	Michelangelo
Miguel Angel	Michelangelo
Microbe	Microbe
Microbes	Microbe
MIKY	MIKY
Mirror	Mirror
Mistake	Fumble-867, Typo Boot
MIX1	MIX1, MIX1-B
MIX1-B	MIX1-B
MIX1/Icelandic	Saratoga 1, Saratoga 2, Iceland II
Mixer1	MIX1
Moctezuma	Moctezuma
Monxla	Vienna-Monxla
Morbus Waiblingen	1813
Mosquito	Mosquito
Mother Fish	Whale
Mshark-889	Mshark-889
MSHerk v2.10	Mshark-889
Multiface	Multiface
Munich	Friday the 13th COM
Murphy	Murphy 1
Murphy 1	Murphy 1
Murphy 2	Murphy 2
Murphy-1	Murphy 1
Murphy-2	Murphy 2
Music	OROPAX
MusicBug	MusicBug
Musician	OROPAX
MYSTIK	Liberty
Mystic 1	Liberty
Nagytud	Turbo-448
New Zealand	Stoned
Nobock	Nobock

Noint	Noint
Nomenclature	Nomenklatura
Nomenklatura	Nomenklatura
NOV17	NOV17
Number of the Beast	V512
Ogre	Disk Killer
Ohio	Ohio
Ohio0	Ohio0
Old Yankee-1	Yankee-1961
Omicron	Flip-2343, Flip-2153
OMICRON Psychoblaster	Flip-2343, Flip-2153
Ontario	Ontario
One-In-Eight	Vienna-648
OROPAX	OROPAX
PADDED	PADDED
Pakistani	Brain
Pakistani Brain	Brain
Palette	1536
Payday	1813-not-13
PC-FLU 2	PC-FLU 2
PCV	PCV
PcVrsDs	PCV
Peking	Yale
Pentagon	Pentagon
Perfume	Perfume-765
Perfume-731	Perfume-731
Perfume-765	Perfume-765
Phoenix	Phoenix-Phoenix
Phoenix-Evil	Phoenix-Evil
Phoenix-Phoenix	Phoenix-Phoenix
Phoenix-Proud	Phoenix-Proud
Ping Pong-B	Bouncing Ball
Ping-Pong	Bouncing Ball
Pixel	Pixel-847
Pixel-277	Pixel-277
Pixel-299	Pixel-299
Pixel-345	Pixel-345
Pixel-740	Pixel-740
Pixel-847	Pixel-847
Pixel-847B	Pixel-847B
Pixel-852	Pixel-852
Plastique 1	Plastique 4.51
Plastique 2	Plastique-Invader
Plastique 4.51	Plastique 4.51
Plastique 4.51-b	Plastique 4.51-b
Plastique 5.21	Plastique 5.21
Plastique Boot	Plastique-Invader
Plastique-2576	Plastique-2576
Plastique-3088	Plastique-3088
Plastique-2900	Plastique-2900
Plastique-Danube	Plastique-Danube
Plastique-Invader	Plastique-Invader
PLO	1813
Pogue	MtE family
Pojer	Pojer
POLIMER	POLIMER
Polimer-2	POLIMER

Possessed	Poss-A
Pregnant	Pregnant
Pretoria	JUNE16
PrintScreen	PrtSc
Print Screen	PrtSc
Proud	Phoenix-Proud
PrtSc	PrtSc
Prudents	Prudents-1210
Prudents-1210	Prudents-1210
PSQR	PSQR-1720
PSQR-1720	PSQR-1720
PS-Stoned	Brunswick
Questo	MtE family
Quit-1992	555 or 555B
QRry	QRry
Quox	Quox
R-11	LOL
Raubkopi	Raubkopi
RCE1049	RCE1049
Red X	Ambulance
RPVS	453
Russian	1813
Sadam	Sadam
San Diego	Stoned
Saratoga	Iceland II, Saratoga 1, Saratoga 2, December 24th
Saratoga 1	Saratoga 1
Saratoga 2	Saratoga 2
Saratoga 3	Iceland II
SAT14	Saturday 14th
Saturday 14th	Saturday 14th
Saturday-the-14th	Saturday 14th
SBC	SBC
Scott's Valley	Slow-2131
Scream-2b	Scream-2b
Search	Den Zuk
Second Austrian	1704
Seoul	Yale
Shake	Shake
Shoe	Brain-Shoe
Shoe_Virus	Brain-Shoe
Shirley	Shirley
Simulate	Simulate
Slayer	VBASIC-B
SLOV2	SLOV2
Slow	Slow-1721
Slow-1721	Slow-1721
Slow-2131	Slow-2131
Smiley Worm Boot	Smiley Worm Boot
Smithsonian	Stoned
Smulders	Criminal
Solano	Solano
South African	Friday the 13th COM
Spanz	Spanz
Sparse	Sparse
Spanish	Traceback-2930
STAF	STAF

Star Dot	Stardot-600
Stardot-600	Stardot-600
Stardot-789	Stardot-789
Stardot-801	Stardot-801
Stealth	4096, EDV, Fish 6, Joshi, Murphy 1
Stink	Stink
Sticky	Sticky
Stoned	Stoned
Stoned III	Noint
Stoned 2	Stoned 2
Stoned-Alberta	Stoned-Alberta
Stoned-ZAPPED	Stoned-ZAPPED
Striker	Striker
Stupid	Do-Nothing, Sadam
Stupid-2	Do-Nothing 2
Stupid Criminal	Criminal
Subliminal	Solano
sUMsDos	1813
Sunday	Sunday, Sunday 2
Sunday 2	Sunday 2
Suomi	Suomi
SuperHacker	Talentless Jerk
sURIV 1.01	April 1st COM
sURIV 2.01	April 1st EXE
Suriv 3.00	Suriv 3.00
Suriv A	April 1st COM, April 1st EXE
Suriv B	Suriv 3.00
SURIV01	April 1st COM
SURIV02	April 1st EXE
SURIV03	Suriv 3.00
SVC 3.1	SVC 3.1
SVC 4.0	SVC 4.0
SVC 5.0	SVC 5.0
SVC 6.0	SVC 6.0
SVIR	SVIR
Swap	Falling Letters Boot
Swedish Disaster	Swedish Disaster
Sylvia	Sylvia
SYSLOCK	SYSLOCK
SYSLOCK-MACHO	SYSLOCK-MACHO
System	Iceland II
T1	1813
Taiwan 1	Taiwan
Taiwan	Taiwan, Taiwan 2
Taiwan 2	Taiwan 2
Taiwan 3	Plastique-2900
Taiwan 4	Plastique-2576
Talentless Jerk	Talentless Jerk
Telecom	Telecom-3700
Telecom-3700	Telecom-3700
Telecom-3784	Telecom-3784
TELEFONICA	Campana
Telefon	Campana
Ten Bytes	9800:0000
TenBytes	9800:0000
Tequila	Tequila
Thanksgiving	1253

Thursday the 12th	Thursday the 12th
Tiny-134	Tiny-134
Tiny-138	Tiny-138
Tiny-143	Tiny-143
Tiny-154	Tiny-154
Tiny-156	Tiny-156
Tiny-158	Tiny-158
Tiny-159	Tiny-159
Tiny-160	Tiny-160
Tiny-163	Kennedy-163
Tiny-167	Tiny-167
Tiny-198	Tiny-198
TiredBoot	TiredBoot
Toothless	W13-A, W13-B
Tony	Tony
Topo	Topo
TP04VIR	TP04VIR
TP06VIR	TP06VIR
TP16VIR	TP16VIR
TP23VIR	TP23VIR
TP24VIR	TP24VIR
TP25VIR	TP25VIR
TP33VIR	TP33VIR
TP34VIR	TP34VIR
TP38VIR	TP38VIR
TP39VIR	Yankee Doodle-2772
TP41VIR	TP41VIR
TP42VIR	TP42VIR
TP44VIR	Yankee Doodle-2885
TP45VIR	TP45VIR
TP46VIR	TP46VIR
Traceback	Traceback-2930, Traceback-3066
Traceback II	Traceback-2930
Traceback-2930	Traceback-2930
Traceback-3066	Traceback-3066
Traveller	Traveller
Tremor	Tremor
Trivial (46)	Minimal-46
Troi	Troi
TUQ	453
Turbo	Turbo-Kukak, Turbo-448
Turbo-448	Turbo-448
Turbo-Kukac	Turbo-Kukak
Turin	Bouncing Ball
Turku	KeyPress
Typo	Fumble-867, Typo Boot
Typo Boot	Typo Boot
Typo COM	Fumble-867
UIUC	Brain-Ashar
UIUC	Brain-Shoe
Ultimate Weapon	Criminal
Unesco	Vienna-648
V-277	Pixel-277
V-299	Pixel-299
V-345	Pixel-345
V-Alert	9800:0000
V08-15	Fingers

V1024	V1024
V1277	Murphy 1
V1539	XA1
V2000	V2000
V2100	Dark Avenger-2100
V2P1	Washburn-1260, Washburn-V2P2 or Washburn-Casper
V2P2	Washburn-1260, Washburn-V2P2 or Washburn-Casper
V512	V512
V512-B	V512-B
V512-C	V512-C
V512-D	V512-D
V512-E	V512-E
V651	Eddie-651
V800	V800
V801	Stardot-789
Vacsina v5	VACSINA
Vacsina v16	TP16VIR
VACSINA	VACSINA
Vacsina-39 Virus	Yankee Doodle-2772
Vacsina-44 Virus	Yankee Doodle-2885
VBASIC	VBASIC
VBASIC-B	VBASIC-B
VCOMM	637
VCS 1.0	VCS 1.0
Venezuelan	Den Zuk
Vera Cruz	Bouncing Ball
VHP-348	VHP-348
VHP-353	VHP-353
VHP-367	VHP-367
VHP-435	VHP-435
VHP-623	VHP-623
VHP-627	VHP-627
VHP-648	VHP-648
Victor	Victor
Vienna	Vienna-648
Vienna 62 A	Vienna-648
Vienna (DOS62) Version B	Vienna-648
Vienna-535	Vienna-535
Vienna-645	Vienna-645
Vienna-646	Vienna-646
Vienna-648	Vienna-648
Vienna-733	Vienna-733
Vienna-Choinka	Vienna-Choinka
Vienna-Ghost	Vienna-Ghost
Vienna-Ira	Vienna-Ira
Vienna-Lisbon	Vienna-Lisbon
Vienna-Monxla	Vienna-Monxla
Vienna-Viola	Vienna-Viola
Vienna-Viola B4	Vienna-Viola B4
Viola	Vienna-Viola
Viola B4	Vienna-Viola B4
Violator	Vienna-Viola
VIR13J	July 13th
Virdem	Virdem
Virdem 2	Virdem 2
VIRUS-90	VIRUS-90
Virus-B	Friday the 13th COM

Voronezh	Voronezh
VP	VP
Vriest	Vriest
V-SIGN	CANSU
W13	W13-A, W13-B
W13-A	W13-A
W13-B	W13-B
Washburn-Casper	Washburn-1260, Washburn-V2P2 or Washburn-Casper
Weinacht	XA1
Westwood	1813-Westwood
Whale	Whale
Whale-B	Whale-B
Witcode	V789
Wisconsin	Wisconsin
Wolfman	Wolfman
XA1	XA1
XA1 (1539) Christmas	XA1
Yale	Yale
Yale Boot	Yale
Yankee 2	Yankee-1961
Yankee Doodle	Yankee Doodle-2885, Yankee Doodle-2772
Yankee Doodle-2772	Yankee Doodle-2772
Yankee Doodle-2885	Yankee Doodle-2885
Yankee-1624	Yankee-1624
Yankee-1961	Yankee-1961
Yaunch	Yaunch
YEKE-1076	YEKE-1076
YEKE-1204	YEKE-1204
YEKE-2425	YEKE-2425
Z the Whale	Whale
ZAPPER	Stoned-ZAPPED
ZBug	1536
Zero Bug	1536
Zero Hunt	Zero Hunt
Zero Hunt-B	Zero Hunt-B
Zerotime	Slow-1721
ZK900	ZK-900
ZK-900	ZK-900
#1	Taunt
100 Years	4096
382	382
405	Burger-405
440	NoBock
453	453
512	V512
537	Burger-537
541	Burger-541
555	555 or 555-B
555-B	555 or 555-B
5X2	Grain of Sand
560	Burger-560
637	637
640k	Do Nothing
648	Vienna-648
648-Lisbon	Vienna-Lisbon
651	Eddie-651
688	FLASH

765	Perfume-765
805	Stardot-789
817	Stardot-801
834	Arab
847	Pixel-847
867	Fumble-867
903	CHV 2.1
920	Datalock
941	Devil's Dance-941
1008	Suomi
1022	Fellowship
1024	V1024
1168	DataCrime-1168
1210	Prudents-1210
1226	Phoenix-1226
1244	1244
1253	1253
1260	Washburn-1260, Washburn-V2P2 or Washburn-Casper
1260-Casper	Washburn-1260, Washburn-V2P2 or Washburn-Casper
1280	DataCrime-1280
1381	1381
1392	1392
1392 (Amoeba)	1392
1514	DataCrime II
1536	1536
1536 (Zero Bug)	1536
1539	XA1
1554	9800:0000
1559	9800:0000
1575	1575
1591	1575
1605	1813-1605
1624	Yankee-1624
1701	1701
1701-Jojo	1701-Jojo
1701-Nodate	1701
1701/1704 - Version B	1701, 1704, 1704-B, 1704-C, 1704-Format, 1704-Y
1704	1704
1704 Format	1704-Format
1704-B	1704-B
1704-C	1704-C
1704-Format	1704-Format
1704-Y	1704-Y
170X	1701, 1704, 1704-B, 1704-C, 1704-Format, 1704-Y
1720	PQSR
1759	1759
17XX	1701, 1704, 1704-B, 1704-C, 1704-Format, 1704-Y
17Y4	1704-Y
1808(EXE)	1813
1813	1813
1813(COM)	1813
1813-00	1813
1813-1605	1813-1605
1813-26th	1813-26th
1813-ANARKIA	1813-ANARKIA
1813-Captrip	1813-Swiss or 1813-Captrip
1813-Frere	1813-Frere

1813-Mendoza	1813
1813-not-13	1813-not-13
1813-Puerto	1813-Puerto
1813-Swiss	1813-Swiss
1813-Tuesday-1st	1813-Tuesday-1st
1813-Tuesday-1st	1813
1813-Westwood	1813-Westwood
1917	DataCrime II-B
1961 (Yankee)	Yankee-1961
1971	Eight Tunes-1971
1971(Eight Tunes)	Eight Tunes-1971
1993	1993
2086	2086
2100	Dark Avenger-2100
2131	Slow-2131
2153 (Flip)	Flip-2153
2343 (Flip)	Flip-2343
2559	Yaunch
2772	Yankee Doodle-2772
2885	Yankee Doodle-2885
2930	Traceback-2930
3066	Traceback-3066
3066/2930 Traceback	Traceback-2930, Traceback-3066
333	Kennedy-333
3445	3445
3551	SYSLOCK
3551 (Syslock)	SYSLOCK
3555	SYSLOCK
3880	Itavir
4096	4096
4711	Perfume-765
5120	VBASIC
889	Mshark-889
9800:0000	9800:0000

Descriptions of some known DOS viruses

This section briefly describes some of the DOS viruses analyzed by IBM. It includes all of the viruses that are widespread in the world as of this writing. It also includes many viruses that are not widespread, but that we have analyzed in order to help stay ahead of the problem.

These descriptions are based on IBM's detailed analysis of the code of each virus. Each virus has been carefully tested to verify its actual behavior.

All of these viruses can be detected when checking disks and diskettes. Viruses that are similar to these viruses will be detected as well. In many cases, even viruses that are not similar to these will be detected as "suspicious" by IBM AntiVirus/DOS.

To view a particular virus description, double-click on its name in the following list.

Aircop
April 1st COM
April 1st EXE
Azusa
Bouncing Ball
Bouncing Ball / 286
Brain
Brunswick
Burger-405
Campana
Campana-B
Cansu
Dark Avenger
DataCrime II
DataCrime II B
DataCrime-1168
DataCrime-1280
December 24th
Den Zuk
Devil's Dance-941
DIR II
Disk Killer
EDV
Flip-2153
Flip-2343
FORM
Friday the 13th COM
Grain of Sand
Guppy
Haifa
Haifa-Motzkin
Iceland II
Joshi
Joshi-00
Kennedy-163
Keypress
Lao Doung
Lehigh I
Liberty

Liberty-B
Liberty-X
Live After Death
Michelangelo
Microbe
MIX1
MIX1-B
Noint
Ohio
OROPAX
Perfume-765
Plastique-Danube
Plastique-Invader
Plastique-2576
Plastique-2900
Plastique 4.51
Plastique 4.51-b
Plastique 5.21
PrtSc
Saratoga 1
Saratoga 2
SBC
Slow-1721
Solano
StarDot-600
StarDot-789
StarDot-801
Stoned
Stoned-C
Sunday
Sunday 2
sURIV 3
Sylvia
SYSLOCK
Tequila
TP16VIR
TP45VIR
Traceback-2930
Traceback-3066
VACSINA
Vienna-Ghost
Vienna-Lisbon
Vienna-648
W13-A
W13-B
Yale
Yankee Doodle-2772
Yankee Doodle-2885
1381
1392
1536
1575
1701
1701-NoDate
1704

1704-B

1704-C

1704-Format

1704-Y

1813

1813-00

1813-ANARKIA

1813-Discom

1813-Not-13

1813-Swiss

1813-Tuesday-the-13th

2086

4096

555

555-B

The Aircop Virus

Name Aircop

Alias(es)

Virus Family

Classification Diskette boot record infector

Length of Virus Boot record and one additional hard disk or diskette sector

Behavior Summary When booted from an infected diskette, the virus loads into memory and infects diskettes used in A: or B: later. Every eight or so times that it infects a new diskette, it displays the message "RED STATE, Germ offensing   --Aircop" (presumably an attempt to say "Condition red, virus attack").

The April 1st COM Virus

Name	April 1st COM
Alias(es)	April 1st, sURIV 1.01
Virus Family	1813
Classification	Resident COM infector
Length of Virus	Approximately 381 bytes

Behavior Summary When an infected program is run, the virus installs itself in memory and any COM files run later become infected. If the date is April 1st of any year, executing any program while the virus is in memory will display the message "APRIL 1ST HA HA HA YOU HAVE A VIRUS", and will hang the machine. If the date is after April 1st, 1988, the message "YOU HAVE A VIRUS" will be displayed whenever any program is executed Because infection is so obvious, this virus is probably extinct.

The April 1st EXE Virus

Name April 1st EXE
Alias(es) April 1st, sURIV 2, sURIV 2.01
Virus Family 1813
Classification Resident EXE infector
Length of Virus 1488 bytes
Behavior Summary This virus infects any EXE files that are run, prints a message on April 1st, and sometimes causes the system to hang on Wednesdays.

The Azusa Virus

Name	Azusa
Alias(es)	
Virus Family	
Classification	Diskette and hard disk boot infector
Length of Virus	Boot record only
Behavior Summary	This virus infects diskette and hard disk master boot record. Sometimes the virus zeros out the BIOS tables for COM and printer ports, making printers and serial ports unavailable.

The Bouncing Ball Virus

Name	Bouncing Ball
Alias(es)	Bouncing Dot, Italian, Ping-Pong, Vera Cruz
Virus Family	Bouncing Ball
Classification	Diskette and hard disk boot infector
Length of Virus	Approximately 975 bytes
Behavior Summary	This virus infects diskettes and the hard disk partition (non-master) boot record. It sometimes produces a bouncing dot on the screen after booting.

The Bouncing Ball / 286 Virus

Name	The Bouncing Ball / 286 Virus
Alias(es)	
Virus Family	Bouncing Ball
Classification	Diskette and hard-disk boot infector
Length of Virus	Approximately 975 bytes
Behavior Summary	This virus infects diskettes and the hard disk partition (non-master) boot record. It sometimes produces a bouncing dot on the screen after booting.

The Brain Virus

Name	Brain
Alias(es)	Pakistani, Pakistani Brain, (c) Brain
Virus Family	Brain
Classification	Diskette boot infector
Length of Virus	Boot record and 6 additional sectors on hard disk or diskette
Behavior Summary	This virus changes some diskette volume labels to "(c) Brain"

The Brunswick Virus

Name	Brunswick
Alias(es)	
Virus Family	
Classification	Resident diskette and hard disk master boot infector
Length of Virus	Boot record and one additional hard disk or diskette sector
Behavior Summary	When you boot from an infected diskette, it infects the first physical hard disk in the system. When you boot from an infected hard disk or diskette, the virus loads into memory and infects diskettes used in drive A or B later. When booting from an infected hard disk, it sometimes overwrites the master boot record with useless data, rendering the disk unbootable. Also, the data becomes inaccessible without technical help. As well as the intentional damage, on some systems the virus overlays user data and possibly part of the file allocation table when it saves the original boot record in the data section of the hard disk.

The Burger-405 Virus

Name	Burger-405
Alias(es)	405
Virus Family	Burger
Classification	COM overwriting virus for IBM DOS
Length of Virus	Overwrites first 405 bytes of victim

Behavior Summary This virus is very buggy, apparently based on a published example. When an infected file is run it overlays the first 405 bytes of every file with an extension of COM in the current directory of various hard disks with a copy of itself. The original (pre infection) program does **not** run. Running an infected program often hangs the machine or otherwise malfunctions.

The Campana Virus

Name Campana
Alias(es) Telefonica, Anti-Telefonica, Telefon, ANTI-CTNE
Virus Family Campana
Classification Resident infector of diskette boot records and hard disk master boot records
Length of Virus Boot record and one additional hard disk or diskette sector
Behavior Summary When a machine is booted from an infected hard disk or diskette, the virus loads itself into high memory and reduces available memory by 1024 bytes. The machine's hard disk (if any) and any diskettes used in drive A or B while the virus is in memory are infected. After a certain number of boots from an infected hard disk or diskette, the virus writes random data to the boot hard disk or diskette and other hard disks in the system and displays a message beginning with the word "Campana". While the virus is in memory, it intercepts most attempts to read the boot record and returns an image of an uninfected boot record to the program making the request.

The Campana-B Virus

Name Campana-B

Alias(es) Telefonica, Anti-Telefonica, Telefon, ANTI-CTNE

Virus Family Campana

Classification Resident infector of diskette boot records and hard disk master boot records

Length of Virus Boot record and one additional hard disk or diskette sector

Behavior Summary When a machine is booted from an infected hard disk or diskette, the virus loads itself into high memory and reduces available memory by 1024 bytes. The machine's hard disk (if any) and any diskettes used in drive A or B while the virus is in memory are infected (unless they are already infected with the Stoned virus). After a certain number of boots from an infected hard disk or diskette, the virus writes random data to the boot hard disk or diskette and other hard disks in the system and display a message beginning with the word "Campana". While the virus is in memory, it intercepts most attempts to read the hard disk boot record and returns an image of an uninfected boot record to the program making the request.

The Cansu Virus

Name Cansu

Alias(es) V-Sign

Virus Family

Classification Resident diskette and hard disk master boot infector

Length of Virus Boot record and 2 additional sectors on hard disk or diskette

Behavior Summary When you boot from an infected hard disk or diskette, the virus loads into memory and infects diskettes used in drive A or B later; Also, it infects the first two physical hard disks in the system when they are used. In approximately one-in-eight-boots, the virus displays a V-shaped symbol on the display. The virus does no intentional damage; but, on some systems, it overlays your data and perhaps part of the file allocation table when it writes its two sectors to the data section of the hard disk.

The Dark Avenger Virus

Name Dark Avenger
Alias(es) Eddie
Virus Family
Classification Resident COM and EXE file virus for IBM DOS
Length of Virus 1800 bytes in infected COM files; some additional padding bytes in infected EXE files.
Behavior Summary When an infected program is run, the virus installs itself in memory. It might infect any EXE or COM file run, opened, renamed, or operated on in some way. So any operation that examines many files can spread the virus very quickly if it is active in memory at the time. Approximately every 16 times an infected program is run, it overwrites a random sector of the disk the program was run from with the string "Eddie lives...somewhere in time!" followed by part of the body of the virus.

The DataCrime II Virus

Name DataCrime II
Alias(es) 1514, Columbus Day
Virus Family DataCrime
Classification Non-resident COM and EXE infector for IBM DOS
Length of Virus 1514 bytes in infected COM files; some additional padding bytes in infected EXE files.
Behavior Summary This virus spreads between COM files. If an infected program is run between October 13th and December 31st, inclusive, in any year, it will display the message "* DATACRIME II VIRUS", and erase part of the hard disk, rendering data inaccessible.

The DataCrime II B Virus

Name DataCrime II B
Alias(es) 1480, Columbus Day
Virus Family DataCrime
Classification Non-resident COM and EXE infector for IBM DOS
Length of Virus 1480 bytes in infected COM files; some additional padding bytes in infected EXE files.
Behavior Summary This virus spreads between COM files. If an infected program is run between October 13th and December 31st, inclusive, in any year, it will display the message "* DATACRIME II VIRUS", and erase part of the hard disk, rendering data inaccessible.

The DataCrime-1168 Virus

Name DataCrime-1168
Alias(es) 1168, Columbus Day, DataCrime, DataCrime I
Virus Family DataCrime
Classification Non-resident COM infector for IBM DOS
Length of Virus 1168 bytes
Behavior Summary This virus spreads between COM files. If an infected program is run between October 13th and December 31st, inclusive, in any year, it will display the message "DATACRIME VIRUS RELEASED: 1 MARCH 1989", and erase part of the hard disk, rendering data inaccessible.

The DataCrime-1280 Virus

Name	DataCrime-1280
Alias(es)	1280, Columbus Day, DataCrime, DataCrime I
Virus Family	DataCrime
Classification	Non-resident COM infector for IBM DOS
Length of Virus	1280 bytes
Behavior Summary	This virus spreads between COM files. If an infected program is run between October 13th and December 31st, inclusive, in any year, it will display the message "DATACRIME VIRUS RELEASED: 1 MARCH 1989", and erase part of the hard disk, rendering data inaccessible.

The December 24th Virus

Name	December 24th
Alias(es)	Disk Crunching, Iceland, Iceland III, Icelandic, Saratoga
Virus Family	Iceland/Saratoga
Classification	Resident EXE infector
Length of Virus	Approximately 848 bytes

Behavior Summary When an infected program is run, the virus installs itself in memory; later, if any file with an extension beginning with "EX" is run, it may be infected. Approximately every tenth file run is infected. The basic code of the virus is similar to the others in the family. This version infects every tenth file run and does not mark sectors as bad. If an infected file is run on December 24th, any attempt to run a program after that will print the message "Gledileg jol", (which is a Christmas greeting in Icelandic) rather than running the program.

The Den Zuk Virus

Name	Den Zuk
Alias(es)	Den Zuko
Virus Family	Ohio
Classification	Diskette boot record infector
Length of Virus	Boot record and 8 additional sectors on hard disk or diskette
Behavior Summary	When you boot from an infected diskette, the virus loads into memory and infects diskettes used in drive A or B later. If the virus finds signs of the Brain virus on a diskette, it will remove the Brain infection before installing itself. If the virus is in memory and a color display is active when you press Ctrl+Alt+Del, the virus will sometimes display a moving graphic "logo" containing the letters "Den Zuk" and a sphere.

The Devil Virus

Name	Devil's Dance-941
Alias(es)	941, Devil's Dance
Virus Family	Devil's Dance
Classification	Resident COM infector for IBM DOS
Length of Virus	941 bytes

Behavior Summary This virus infects all COM files in the current directory when first invoked. The virus's resident part then infects any file that is run whose extension begins with "C". Sometimes the virus changes the colors of characters typed on a color display. Also, when Ctrl+Alt+Del is pressed it sometimes displays the message "Have you ever danced with the devil under the weak light of the moon?   Pray for your disk!   The_Joker... Ha Ha Ha Ha Ha Ha Ha Ha Ha Ha" Then the virus sometimes overlays the master boot record of the first hard disk with random data.

The DIR II Virus

Name DIR II
Alias(es) DIR 2, Cluster
Virus Family
Classification Cluster virus; resident EXE and COM infector
Length of Virus 1024 bytes (but see below)
Behavior Summary When an infected program is run, the virus installs itself in the DOS device driver chain and infects any hard disk or diskette used later. When the virus infects a disk, it writes one copy of itself to a usually unused part of the disk and redirects the directory entries for all the programs on the disk to point to that copy. The virus does not appear to be destructive; but because it installs itself in the system at a very low level, it often interacts badly with other software, sometimes leading to malfunctions and data loss.

The Disk Killer Virus

Name Disk Killer
Alias(es) Computer Ogre, Disk Ogre, Ogre
Virus Family Disk Killer
Classification Diskette and hard -disk (DOS) boot infector
Length of Virus Boot record and 4 additional sectors on hard disk or diskette
Behavior Summary This virus infects diskette boot records and hard disk non-master (DOS) boot records. About 48 hours after booting from an infected hard disk or diskette, the message "Disk Killer -- Version 1.00 by COMPUTER OGRE 04/01/89 Warning!!! Don't turn off the power or remove the diskette while Disk Killer is Processing!" is displayed, and data on the disk booted from (or whatever disk is in the diskette you drive booted from) is scrambled.

The EDV Virus

Name EDV
Alias(es)
Virus Family
Classification Diskette and fixed disk master boot infector
Length of Virus Boot record and one additional hard disk or diskette sector
Behavior Summary When booted from an infected disk or diskette, the virus loads into memory and infects any other disks or diskettes used later. When an internal counter reaches a threshold, the virus overwrite areas on various fixed disks and diskettes with random data. Due to bugs in the virus, and code that attempts to hang the machine when memory is scanned, infected machines sometimes malfunction (not boot, or hang sometime after booting). If a machine with an infected fixed disk is booted from a clean diskette, the fixed disk partitions will often be unreadable by DOS.

The Flip-2153 Virus

Name Flip-2153
Alias(es) Flip 2, Omicron
Virus Family Flip
Classification IBM DOS EXE, COM, and master boot record infector
Length of Virus Approximately 2153 bytes
Behavior Summary When an infected file is executed on a machine with a hard disk, the hard disk's master boot record is altered to reinstall the virus in memory even if all infected files are removed. While the virus is in memory, any file executed becomes infected. On some second days of the month between 10:00 and 11:00 a.m., the screen (including the individual characters) turns upside-down if an EGA-compatible display is in use.

The Flip-2343 Virus

Name	Flip-2343
Alias(es)	Flip 1, Flip
Virus Family	Flip
Classification	IBM DOS EXE, COM, and master boot record infector
Length of Virus	Approximately 2343 bytes

Behavior Summary When an infected file is executed on a machine with a hard disk, the hard disk's master boot record is altered to re install the virus in memory even if all infected files are removed. When a system is booted from an infected hard disk, the next program executed (typically COMMAND.COM) is patched. In at least some versions of COMMAND.COM, the patch causes the DIR command to "lie" about the lengths of infected files. While the virus is in memory, any file executed becomes infected. On some second days of the month between 10:00 and 11:00 a.m., the screen (including the individual characters) turns upside-down if an EGA-compatible display is in use.

The FORM Virus

Name FORM
Alias(es)
Virus Family
Classification Resident diskette and hard disk DOS boot infector
Length of Virus Boot record and one additional hard disk or diskette sector
Behavior Summary When you boot from an infected diskette or hard disk, the virus infects the bootable partition on the first hard disk if it exists and if is not already infected. Also, it writes part of itself to one additional sector marked "bad" in the File Allocation Table. The virus remains resident in memory and infects essentially any diskette used later. On the 18th of the month, in machines with a normal real time clock, the virus causes a slight clicking when keys are pressed which often goes unnoticed.

If you boot an OS/2 system with HPFS on the boot drive from an infected diskette, some of the data can become corrupted and the system will no longer boot from the hard disk.

The Friday the 13th COM Virus

Name Friday the 13th COM
Alias(es) COM, Friday the 13th, Miami, Munich, South African, Virus-B
Virus Family
Classification Non-resident COM infector
Length of Virus Approximately 540 bytes
Behavior Summary When an infected program is run, it infects all COM files in the current directory. On Friday the 13th, infected files attempt to erase themselves when executed. This virus has an indefinite history. It might have been written only as an experiment and not released "into the wild." The sample we have contains code that prints a warning message whenever an infected program is run.

The Grain of Sand Virus

Name Grain of Sand
Alias(es) Irish, Maltese Amoeba
Virus Family
Classification Resident EXE and COM infector
Length of Virus Approximately 2520 bytes
Behavior Summary When an infected program is executed, the virus installs itself in memory and infects files that are later executed or opened. When the date is November 1 or March 15, it also overwrites the boot areas of the first hard disk and any diskettes with a program that displays a poem (containing the words "grain of sand") instead of booting the machine. Data on infected disks and diskettes is not easy to recover. After it overwrites the boot areas, it hangs the machine, sometimes with a flashing screen-effect on the display. The virus is loosely related to the Casino virus, which does not install itself if the Grain of Sand is active. If the Grain of Sand finds the Casino present in memory, it will attempt to remove it.

The Guppy Virus

Name	Guppy.
Alias(es)	None.
Virus Family	Tiny.
Classification	Resident COM and EXE file virus for PC DOS
Length of Virus	152 bytes
Behavior Summary	When an infected program is executed, the virus loads into memory and infects COM files that are run later.

The Haifa Virus

Name Haifa
Alias(es)
Virus Family Haifa
Classification Resident COM and EXE infector for IBM DOS
Length of Virus Approximately 2350 bytes
Behavior Summary When an infected file is run, the virus loads into memory and infects COM and EXE files found in directories that are used later. Also, it hangs the machine periodically, prints a message on August 24th and on April 8th, and inserts text strings into certain types of files found. It inserts a text string containing "mov dx,80h" into files with an extension of ASM. It inserts a text string containing "CONST VIRUS=" into files with an extension of PAS. It inserts a text string beginning "OOPS! Hope I" into files with an extension of DOC or TXT.

The Haifa-Motzkin Virus

Name	Haifa-Motzkin
Alias(es)	Motzkin, Mozkin
Virus Family	Haifa
Classification	Resident COM and EXE infector for IBM DOS
Length of Virus	Approximately 2350 bytes

Behavior Summary When an infected file is run, the virus loads into memory, and infects COM and EXE files found in directories that are used later. Hangs the machine periodically, prints a message on May 7th, and inserts text strings into certain types of files found; it might also sometimes cause unexpected screen printing. It inserts a text string containing "What are backups" into files with an extension of BAK. It also inserts a text string containing "DES of USA" into files with an extension of ARJ. It also inserts a text string containing "Instead of reading this" into files with an extension of DOC or TXT.

The Iceland II Virus

Name	Iceland II
Alias(es)	Iceland, Icelandic, Icelandic II, Saratoga, Saratoga 3, System
Virus Family	Iceland/Saratoga
Classification	Resident EXE infector
Length of Virus	Approximately 632 bytes

Behavior Summary When an infected program is run, the virus installs itself in memory; later, if any file with an extension beginning with "EX" is run it will be infected. This virus differs from the Saratoga 1 in that it does not mark sectors as bad. It avoids using INT 21 to call DOS by finding the "true" DOS function-request entry point and thereby avoiding detection by any anti-virus program that relies on intercepting INT 21.

The Joshi Virus

Name	Joshi
Alias(es)	
Virus Family	Joshi
Classification	Resident diskette and hard disk master boot infector
Length of Virus	Boot record and 8 additional sectors on hard disk or diskette

Behavior Summary On January 5th, infected machines display the message "Type Happy Birthday Joshi!", and freeze until "happy birthday joshi" is typed on the keyboard. When an infected hard disk or diskette is booted, the virus loads itself into high memory and intercepts the keyboard, timer, disk, and (a bit later) DOS service call vectors. The viral disk I/O handler infects the boot record of BIOS drives 00, 01, 80 and 81 (drives A, B, and the first two physical hard disks) when I/O is done to those drives. It also hides the viral boot record from normal reads, returning an image of the original boot record. The keyboard handler is used by the virus to remain in memory when a soft (Ctrl+Alt+Del) reboot is done. The DOS service call handler is used to choose a good time to activate if the date is January 5th.

On infected diskettes, the virus resides in the boot record and in a specially formatted extra track that the virus creates. Using DISKCOPY or other normal disk-imaging or disk-copying tools does **not** make a true image of the infected diskette (most of the virus and the original boot record will be missing). Virus verification tools tell you that such a diskette is not infected with the normal Joshi virus.

If a hard disk that was partitioned by a version of FDISK prior to DOS version 3.0 becomes infected, the virus will overwrite part of the File Allocation Table with part of itself. This is true regardless of the version of DOS actually installed on the disk at the time of infection. The only determining factor is the version of FDISK last used to partition the drive. When the disk is not very full, this does not cause noticeable symptoms for some time. When the disk is full, it causes extensive file cross-linking and corruption.

The Joshi-00 Virus

Name	Joshi-00
Alias(es)	
Virus Family	Joshi
Classification	Resident diskette and hard disk master boot infector
Length of Virus	Boot record and 8 additional sectors on hard disk or diskette

Behavior Summary On January 5th, infected machines display the message "Type Happy Birthday Joshi!", and freeze until "happy birthday joshi" is typed on the keyboard. When an infected hard disk or diskette is booted, the virus loads itself into high memory and intercepts the keyboard, timer, disk, and (a bit later) DOS service call vectors. The viral disk I/O handler infects the boot record of BIOS drives 00, 01, 80 and 81 (drives A, B, and the first two physical hard disks) when I/O is done to those drives. It also hides the viral boot record from normal reads, returning an image of the original boot record. Although this version of the virus is slightly damaged and it might be possible to read the viral boot record with a clever use of VERIFY, this has not been tested. The keyboard handler is used by the virus to remain in memory when a soft (Ctrl+Alt+Del) reboot is done. The DOS service call handler is used to choose a good time to activate if the date is January 5th.

On infected diskettes, the virus resides in the boot record and in a specially formatted extra track that the virus creates. Using DISKCOPY or other normal disk-imaging or disk-copying tools does **not** make a true image of the infected diskette (most of the virus and the original boot record will be missing). Virus verification tools tell you that such a diskette is not infected with the normal Joshi virus.

If a hard disk that was partitioned by a version of FDISK prior to DOS version 3.0 becomes infected, the virus will overwrite part of the File Allocation Table with part of itself. This is true regardless of the version of DOS actually installed on the disk at the time of infection. The only determining factor is the version of FDISK last used to partition the drive. When the disk is not very full, this does not cause noticeable symptoms for some time. When the disk is full, it causes extensive file cross-linking and corruption.

The Joshi-00 is a variant of the Joshi virus. One word has been overwritten with binary zeros, which has little or no effect on the function of the virus.

The Kennedy-163 Virus

Name	Kennedy-163
Alias(es)	Tiny-163
Virus Family	Kennedy
Classification	Non-resident COM file virus for IBM DOS
Length of Virus	163 bytes
Behavior Summary	This virus does nothing except infect COM files.

The Keypress Virus

Name Keypress

Alias(es) Turku

Virus Family

Classification Resident COM and EXE file virus for IBM DOS

Length of Virus Approximately 1232 bytes

Behavior Summary When an infected file is executed, the virus loads into memory. If the active version of DOS is 3.0 or later, it will infect all files executed later. If the active version of DOS is earlier than 3.0, it infects all files having an extension of COM or EXE that are opened, except system files. At intervals of 10 minutes, the virus causes spurious simulated keystrokes for a period of 2 seconds and causes the keyboard to appear "stuck".

The Lao Doung Virus

Name	Lao Doung
Alias(es)	Loa Doung, Lao Duong
Virus Family	
Classification	Resident diskette and hard disk system (non-master) boot infector
Length of Virus	Boot record and one additional hard disk or diskette sector

Behavior Summary When an infected disk or diskette is booted, the virus installs itself in memory. When booted from diskette, it attempts to infect the boot record of the first partition on the first fixed disk. When the virus is in memory, it occasionally plays "music" through the PC speaker (our correspondants in Thailand tell us that the tune is an old folk song called Lao Doung Duen).

Due to assumptions made about the setup of hard disks, the virus might fail to infect and/or might damage data on some hard disks.

The Lehigh I Virus

Name Lehigh I
Alias(es)
Virus Family Lehigh
Classification Resident COMMAND.COM infector (IBM DOS)
Length of Virus Approximately 530 bytes
Behavior Summary This virus spreads between COMMAND.COM files. On the fourth infection, it writes random data to lower the 32 sectors of the disk, making files on them inaccessible. Infected COMMAND.COM files do not change in length because the virus writes itself over buffer space within the file.

The Liberty Virus

Name	Liberty
Alias(es)	Mystic
Virus Family	Liberty
Classification	Resident COM, EXE, and diskette boot infector for IBM DOS
Length of Virus	Approximately 2857 bytes

Behavior Summary When an infected file is run, the virus loads into memory and infects EXE and COM files that are later executed. Rarely does the virus also infect the boot record of a diskette. When you boot from an infected diskette the virus installs itself in memory to infect COM and EXE files, and also installs a number of "prank" routines that sometimes replace text sent to the screen, the printer, or the asynchronous communication ports with the word "MAGIC". Also on rare occasions displays "M A G I C ! ! !" on the first line of the screen momentarily.

The Liberty-B Virus

Name	Liberty-B
Alias(es)	Mystic
Virus Family	Liberty
Classification	Resident COM, EXE, and diskette boot infector for IBM DOS.
Length of Virus	Approximately 2867 bytes
Behavior Summary	When an infected file is run, the virus loads into memory and infects EXE and COM files that are later run. Rarely does the virus infect the boot record of a diskette. When you boot with an infected diskette, the virus installs itself in memory to infect COM and EXE files and also installs a number of "prank" routines. This is a slight, functionally identical variant of the Liberty virus.

The Liberty-X Virus

Name	Liberty-X
Alias(es)	Mystic
Virus Family	Liberty
Classification	Resident COM and EXE infector for IBM DOS
Length of Virus	Approximately 2857 bytes

Behavior Summary When an infected file is run,the virus loads into memory and infects EXE and COM files that are later run. This is a damaged variant of the Liberty virus, which cannot infect diskettes, and does not contain the "prank" code from the Liberty virus. In circumstances where the Liberty would infect a diskette, the Liberty-X malfunctions, generally hanging the system.

The Live After Death Virus

Name Live After Death
Alias(es) V810
Virus Family V800
Classification Resident COM infector for IBM DOS
Length of Virus 810 bytes
Behavior Summary This virus infects only COM files of specific lengths. It attempts to intercept DOS requests at a low level in order to avoid detection by security programs.

The Michelangelo Virus

Name Michelangelo
Alias(es)
Virus Family
Classification Diskette and hard disk master boot-record infector
Length of Virus Boot record and one additional hard disk or diskette sector
Behavior Summary When booted from diskette, this virus infects the master boot record of the first hard disk (if any) and installs the virus in memory. When booted from an infected hard disk, it only installs the virus in memory. While the virus is in memory, diskettes used in drive A become infected. If the date is March 6th when you boot from an infected disk or diskette is the virus will overwrite parts of the boot disk with random data.

The Microbe Virus

Name	Microbe
Alias(es)	Microbes
Virus Family	
Classification	Resident diskette boot infector
Length of Virus	Boot record and 8 additional sectors on hard disk or diskette
Behavior Summary	When you boot from an infected diskette, the virus installs itself in memory and infects any writeable diskette used in drives A or B later. If a diskette is infected with the Brain virus, it will remove the Brain infection before installing itself. While the virus is active in memory, attempts to read or write to an infected boot record are redirected to the saved original boot record instead. The virus uses eight sectors (four clusters) on diskette, which it marks as "bad" in the DOS File Allocation Table. If the virus has been booted a large number of times, it will display during the boot process a message that begins "This MICROBE is dedicated to...".

The MIX1 Virus

Name	MIX1
Alias(es)	
Virus Family	Iceland/Saratoga
Classification	Resident EXE infector
Length of Virus	Approximately 1618 bytes
Behavior Summary	When an infected program is run, the virus installs itself in memory; later, if any file with an extension beginning with "EX" is run, it will be infected. This virus differs from the Saratoga 1 in that it does not mark sectors as bad, and it contains code to cause errors (character substitutions) in serial and printer output using BIOS, and to cause a bouncing ball to appear on the screen in some conditions. The bouncing ball code appears to have a bug that sometimes hangs the machine.

The MIX1-B Virus

Name	MIX1-B
Alias(es)	
Virus Family	Iceland/Saratoga
Classification	Resident EXE infector
Length of Virus	Approximately 1618 bytes

Behavior Summary When an infected program is run, the virus installs itself in memory; later, if any file with an extension beginning with "EX" is run, it will be infected. The virus contains code to cause errors (character substitutions) in serial and printer output using BIOS and to cause a bouncing ball to appear on the screen in some conditions. Some of the errors in the MIX1 virus seem to be fixed in this variant.

The Noint Virus

Name Noint
Alias(es)
Virus Family
Classification Diskette and hard disk master boot record infector.
Length of Virus Approximately 420 bytes
Behavior Summary When booted from diskette, the virus infects the master boot record of the first hard disk (if any) and installs the virus in memory. When booted from an infected hard disk, it only installs the virus in memory. While the virus is in memory, any (not write protected) diskettes read from become infected. If the virus is active in memory, attempts to read the infected boot record from the first hard disk will see the original uninfected boot record instead. The virus has no intentional side-effects, destructive or otherwise.

The Ohio Virus

Name Ohio
Alias(es)
Virus Family Ohio
Classification Diskette boot record infector
Length of Virus Boot record and 5 additional sectors on hard disk or diskette
Behavior Summary When you boot from an infected diskette, the virus loads into memory and infects diskettes used in drive A or B later. If the virus finds signs of the Brain virus on a diskette, it will remove the Brain infection before installing itself. If the virus is in memory and a color display is active when the user presses Ctrl+Alt+Del, the virus will sometimes hang the machine. It seems to be designed to display a graphic, similar to the Den Zuk virus to which it is closely related. In all samples seen so far, the graphic code is missing and the system hangs.

The OROPAX Virus

Name OROPAX
Alias(es)
Virus Family
Classification Resident COM infector for IBM DOS
Length of Virus Approximately 2765 bytes
Behavior Summary When an infected file is executed, the virus installs itself in memory. At certain times later (such as creation of a file or subdirectory. And renaming of a file), the virus infects one additional file having an extension of COM. Infected files can grow by as much as 2815 bytes. Under some circumstances, the virus causes music to play from the PC's speaker (although on some machines the music is never played, in spite of the infection).

The Perfume-765 Virus

Name Perfume-765
Alias(es) 4711
Virus Family
Classification Resident COM infector for IBM DOS
Length of Virus Approximately 765 bytes
Behavior Summary When an infected file is run, the virus installs itself in memory, and any file with an extension of COM that is run later is infected. After a certain number of files have been infected, running an infected program causes a message to be displayed, and execution continues only if you type "4711". In the sample of the virus we have, the message area has been overlayed with zeros and other binary values. There are text variants where the message says something intelligible.

The Plastique-Danube Virus

Name Plastique-Danube
Alias(es) Plastique, Invader, Anticad 4.Danube
Virus Family Plastique, 1813
Classification Resident COM, EXE, diskette, and partition boot sector infector for IBM DOS
Length of Virus Approximately 4096 bytes
Behavior Summary When an infected file is run, the virus loads into memory and infects EXE and COM files that are later run or opened as read-only, and infects the partition (DOS) boot sector on diskettes and hard disks that are later read from. When the virus is active in memory, it sometimes slows down the machine, sometimes plays the Blue Danube Waltz through the PC speaker, and sometimes causes hard disk and diskette writes to fail (after a certain number of keystrokes without a hard disk or diskette write). Under various circumstances involving whether or not you have run ACAD.EXE, the number of keystrokes since the last hard disk write, and the user pressing Ctrl+Alt+Del, the virus hangs the system, sometimes after writing garbage to the first two diskettes or the first two physical hard disks. This virus is closely related to the other members of the Plastique family, especially the Plastique 5.21 and the Plastique-Invader viruses.

The virus also removes the "Disk Killer" virus from hard disks and diskettes that it infects and attempts to disable that virus if it is resident in memory.

The Plastique-Invader Virus

Name Plastique-Invader
Alias(es) Plastique, Invader, Anticad 4.Mozart
Virus Family Plastique, 1813
Classification Resident COM, EXE, diskette, and partition boot sector infector for IBM DOS
Length of Virus Approximately 4096 bytes
Behavior Summary When an infected file is run, the virus loads into memory and infects EXE and COM files that are later run or opened as read-only, and infects the partition (DOS) boot sector on diskettes and hard disks that are later read from. When the virus is active in memory, it sometimes slows down the machine, sometimes plays the theme from the first movement of Mozart's 40th through the PC speaker, and sometimes causes hard disk or diskette writes to fail (after a certain number of keystrokes without a hard disk or diskette write). Under various circumstances involving whether or not you have run ACAD.EXE, the number of keystrokes since the last disk write, and wether you press Ctrl+Alt+Del, the virus hangs the system, sometimes after writing garbage to the first two diskettes or to the first two physical hard disks. This virus is closely related to the other members of the Plastique family, especially the Plastique 5.21 and the Plastique-Danube viruses.

The virus also removes the "Disk Killer" virus from hard disks and diskettes that it infects and attempts to disable that virus if it is resident in memory.

The Plastique-2576 Virus

Name	Plastique-2576
Alias(es)	Plastique, Anticad, Anticad 5, Taiwan 4
Virus Family	Plastique, 1813
Classification	Resident COM and EXE infector for IBM DOS
Length of Virus	Approximately 2576 bytes
Behavior Summary	When an infected file is run the virus loads into memory and infects EXE and COM files that are later run. When the virus is active in memory, it will sometimes slows down the machine, and sometimes plays music through the PC speaker. If you run a file called ACAD.EXE, it will be overwritten with garbage and erased instead. Much of the code in this virus is taken from the 1813 virus, but many of the 1813 virus's symptoms (such as EXE re-infection, file erasure on Friday the 13th, black boxes) have been removed.

The Plastique-2900 Virus

Name	Plastique-2900
Alias(es)	Plastique, Anticad, Anticad 2, Taiwan 3
Virus Family	Plastique, 1813
Classification	Resident COM and EXE infector for IBM DOS
Length of Virus	Approximately 2900 bytes

Behavior Summary When an infected file is run the virus loads into memory and infects EXE and COM files that are later run or opened as read-only. When the virus is active in memory, it sometimes slows down the machine, sometimes plays music through the PC speaker, and sometimes causes hard disk and diskette writes to fail (after a certain number of keystrokes without a hard disk and diskette write). If you execute a file called ACAD.EXE, or press Ctrl+Alt+Del under certain circumstances, the virus hangs the system, sometimes after writing garbage to the first two diskettes and the first two physical hard disks. Much of the code in this virus is taken from the Plastique-2576 virus.

The Plastique 4.51 Virus

Name Plastique 4.51
Alias(es) Plastique, Anticad, Anticad 3.a
Virus Family Plastique, 1813
Classification Resident COM and EXE infector for IBM DOS
Length of Virus Approximately 3012 bytes
Behavior Summary When an infected file is run, the virus loads into memory and infects EXE and COM files that are later run or open as read-only. When the virus is active in memory, it sometimes slows down the machine, sometimes plays music through the PC speaker, and sometimes causes hard disk and diskette writes to fail (after a certain number of keystrokes without a hard disk and diskette write). Under various circumstances involving whether or not you have run a file called ACAD.EXE, the number of keystrokes since the last disk write, and wether you press Ctrl+Alt+Del, the virus hangs the system, sometimes after writing garbage to the first two diskette or the first two physical hard disks. Much of the code in this virus is taken from the Plastique-2900 virus.

The Plastique 4.51-b Virus

Name Plastique 4.51-b
Alias(es) Plastique, Anticad, Anticad 3.b
Virus Family Plastique, 1813
Classification Resident COM and EXE infector for IBM DOS
Length of Virus Approximately 3004 bytes
Behavior Summary When an infected file is run, the virus loads into memory and infects EXE and COM files that are later run or opened as read-only. When the virus is active in memory, it sometimes slows down the machine, sometimes plays music through the PC speaker, and sometimes causes hard disk and diskette writes to fail (after a certain number of keystrokes without a hard disk and diskette write). Under various circumstances involving whether or not you have run a file called ACAD.EXE, the number of keystrokes since the last hard disk write, and wether you press Ctrl+Alt+Del, the virus hangs the system, sometimes after writing garbage to the first two diskettes or the first two physical hard disks. This virus is nearly identical to the Plastique 4.51 virus.

The Plastique 5.21 Virus

Name Plastique 5.21
Alias(es) Plastique, Anticad, Anticad 1.b
Virus Family Plastique, 1813
Classification Resident COM, EXE, diskette, and partition boot sector infector for IBM DOS
Length of Virus Approximately 4096 bytes
Behavior Summary When an infected file is run, the virus loads into memory and infects EXE and COM files that are later run or opened as read-only, and the partition (DOS) boot sector on diskettes and hard disks that are later read from. When the virus is active in memory, it sometimes slows down the machine, sometimes plays music through the PC speaker, and sometimes causes hard disk and diskette writes to fail (after a certain number of keystrokes without a hard disk and diskette write). If the you run a program called ACAD.EXE, the virus will print a warning message. Under various circumstances involving whether or not you have run ACAD.EXE, the number of keystrokes since the last hard disk write, and wether you press Ctrl+Alt+Del, the virus hangs the system, sometimes after writing garbage to the first two diskettes or the first two physical hard disks. Much of the code in this virus is taken from the Plastique-2900 virus.

The virus also removes the "Disk Killer" virus from hard disks and diskettes that it infects, and attempts to disable that virus if it is resident in memory.

The PrtSc Virus

Name PrtSc
Alias(es) Print Screen
Virus Family
Classification Resident diskette and hard disk system (non-master) boot infector
Length of Virus Boot record only
Behavior Summary When you boot from an infected hard disk or diskette, the virus installs itself in memory and infects any diskette and the boot sector of the first partition of any hard disk read later. At intervals, the virus causes a false INT 5 that usually causes the contents of the screen to be printed on the local printer (the same as pressing the Print Screen key).

Because of assumptions made about the setup of hard disks, the virus can fail to infect or damage data on some hard disks.

The Saratoga 1 Virus

Name	Saratoga 1
Alias(es)	Disk Crunching, Iceland, Icelandic, Saratoga
Virus Family	Iceland/Saratoga
Classification	Resident EXE infector
Length of Virus	Approximately 642 bytes
Behavior Summary	When an infected program is run, the virus installs itself in memory; later, if any file with an extension beginning with "EX" is run it will be infected. On certain types of hard disks, randomly chosen sectors are marked gradually as "bad".

The Saratoga 2 Virus

Name	Saratoga 2
Alias(es)	Disk Crunching, Iceland, Icelandic, Saratoga
Virus Family	Iceland/Saratoga
Classification	Resident EXE infector
Length of Virus	Approximately 656 bytes
Behavior Summary	When an infected program is run, the virus installs itself in memory; later, if any file with an extension beginning with "EX" is run it will be infected. On certain types of hard disks, randomly chosen sectors are marked gradually as "bad". This virus differs from the Saratoga 1 in that it does not install itself if any program has intercepted the BIOS disk I/O request.

The SBC Virus

Name SBC
Alias(es)
Virus Family
Classification Resident EXE and COM infector
Length of Virus Approximately 2845 bytes
Behavior Summary When an infected program is executed, the virus installs itself in memory and infects files that are later executed or opened. The length changes caused by the virus are not obvious if the virus is active in memory. The output of the DIR command shows the original uninfected lengths.

The Slow-1721 Virus

Name	Slow-1721
Alias(es)	Slow
Virus Family	Slow, 1813
Classification	Resident COM and EXE infector for IBM DOS
Length of Virus	Approximately 1721 bytes
Behavior Summary	When an infected file is run, the virus loads into memory and infects files that are later run. On some Fridays, the virus sets to zero the timestamps of files written to.

The Solano Virus

Name Solano
Alias(es) Dyslexia V2.01
Virus Family
Classification Resident COM infector for IBM DOS
Length of Virus 2000 bytes
Behavior Summary When an infected file is run, the virus loads into memory and infects COM files (except COMMAND.COM) that are later run. While the virus is resident in memory, on rare occasions it swaps a pair of adjacent digits on the display screen.

The StarDot-600 Virus

Name StarDot-600

Alias(es)

Virus Family StarDot

Classification Non-resident EXE infector for IBM DOS

Length of Virus 600 bytes in infected COM files; some additional padding bytes in infected EXE files.

Behavior Summary When an infected file is run, the virus chooses from the files on the default drive an uninfected EXE file with the "archive" bit on and infects that file. If the day of the week is equal to the value of an internal counter, the virus will also overwrite random areas on the current disk drive and will send random bytes to the I/O ports associated with system devices, such as printers and displays.

The StarDot-789 Virus

Name StarDot-789
Alias(es)
Virus Family StarDot
Classification Non-resident COM and EXE infector for IBM DOS
Length of Virus Approximately 789 bytes
Behavior Summary When an infected file is run, the virus chooses from the files on the default drive an uninfected EXE or COM file with the "archive" bit on and infects that file. If the date is February 13th and the time is after 1 p.m. when an infected file is run, it will overwrite the beginning of every hard disk in the system starting with Z. This virus is functionally identical to the StarDot-801 virus.

The StarDot-801 Virus

Name StarDot-801
Alias(es)
Virus Family StarDot
Classification Non-resident COM and EXE infector for IBM DOS
Length of Virus Approximately 801 bytes
Behavior Summary When an infected file is run, the virus chooses from the files on the default drive an uninfected EXE or COM file with the "archive" bit on and infects that file. If the date is February 13th and the time is after 1 p.m. when an infected file is run, it will overwrite the beginning of every hard disk in the system, starting with Z. This virus is functionally identical to the StarDot-789 virus.

The Stoned Virus

Name	Stoned
Alias(es)	Hawaii, Marijuana, New Zealand, San Diego, Smithsonian
Virus Family	
Classification	Diskette and hard disk boot infector
Length of Virus	Boot record and one additional hard disk or diskette sector

Behavior Summary When a computer is booted from an infected diskette, the virus infects the master boot record of the first physical hard disk, installs itself in memory, and sometimes displays the message "Your PC is now Stoned!" When a computer is booted from an infected hard disk, the virus also installs itself in memory but does not display the message. When the virus is in memory, any diskette used in drive A may become infected. The virus has no intentionally destructive features but causes FAT damage and possible data loss on hard disks partitioned in certain ways.

The Stoned-C Virus

Name Stoned-C
Alias(es) Hawaii, Marijuana, New Zealand, San Diego, Smithsonian
Virus Family Stoned
Classification Diskette and hard-disk boot infector
Length of Virus Boot record and one additional hard disk or diskette sector
Behavior Summary This virus infects diskettes and hard disk master boot record. There are no obvious symptoms. This is a variant of the Stoned virus with the message removed.

The Sunday Virus

Name Sunday
Alias(es)
Virus Family 1813
Classification Resident COM and EXE file virus for IBM DOS
Length of Virus 1636 bytes in infected COM files; some additional padding bytes in infected EXE files.
Behavior Summary This virus is similar to the 1813 virus, except the file-erasing trick is done only on Sundays after 1989. The slow-down and box-scrolling are replaced with a routine that sometimes prints a message about going out and having some fun. This message is displayed only on Sundays after 1989.

The Sunday 2 Virus

Name Sunday 2
Alias(es)
Virus Family 1813
Classification Resident COM and EXE file virus for IBM DOS
Length of Virus 1733 bytes in infected COM files; some additional padding bytes in infected EXE files.
Behavior Summary This virus is similar to the 1813 virus except the file-erasing trick is done only on Sundays after 1989. The slow-down and box-scrolling are replaced with a routine that sometimes prints a message about going out and having some fun. This message is displayed only on Sundays after 1989. Also, the virus sometimes writes the word "PLAY" in the upper-left corner of the display.

The sURIV 3.00 Virus

Name sURIV 3.00
Alias(es) Jerusalem-2E
Virus Family 1813
Classification Resident COM and EXE file virus for IBM DOS
Length of Virus 1813 bytes in infected COM files; some additional padding bytes in infected EXE files.
Behavior Summary This virus erases files executed on Fridays and causes some odd system behavior. It is similar to the 1813 virus.

The Sylvia Virus

Name Sylvia
Alias(es) Holland Girl
Virus Family
Classification Non-resident COM infector for IBM DOS
Length of Virus Approximately 1332 bytes
Behavior Summary When an infected file is run, it infects up to 5 files with an extension of COM in the current directories on the current drive and on drive C. The virus has no known side effects. It gets its name from the presence of an unused text area containing a name and address of someone named Sylvia from the Netherlands plus a suggestion to send her a funny postcard.

The SYSLOCK Virus

Name	Syslock
Alias(es)	Macho, Macho-A, 3551
Virus Family	Syslock
Classification	Non-resident COM and EXE infector for IBM DOS
Length of Virus	3551 bytes

Behavior Summary When an infected file is run, the virus looks through the directory tree on the current drive and infects one EXE or COM file at random. Sometimes (approximately every fifth time it runs), it picks a random sector on the current disk and changes all occurrences of the string "Microsoft" to "MACROSOFT". Also a text variant exists that uses "MACHOSOFT" instead of "MACROSOFT."

The Tequila Virus

Name Tequila
Alias(es)
Virus Family
Classification Resident EXE and hard disk master boot infector for IBM DOS
Length of Virus Approximately 2470 bytes
Behavior Summary When an infected file is run, it infects the master boot record of the first hard disk. When a system is booted from an infected hard disk, the virus loads into memory and infects any EXE files subsequently run. The virus displays a low-resolution Mandelbrot set (a vaguely circular pattern of colors) on the monitor. The virus has a number of complex, but basically uninteresting, features having to do with not infecting files with certain names, trying to escape detection by making each infected file slightly different, and so on. From your point of view, though, detection is not difficult.

The TP16VIR Virus

Name	TP16VIR
Alias(es)	
Virus Family	TPxxVIR
Classification	Resident EXE-converter and COM infector for IBM DOS
Length of Virus	Approximately 1339 bytes
Behavior Summary	This virus converts EXE-formatted files to COM format and infects COM-formatted files. The virus becomes resident when the first infected file is run and converts or infects any files that are run later. This virus is similar to the VACSINA virus.

The TP45VIR Virus

Name TP45VIR
Alias(es) Yankee Doodle, TP45
Virus Family Yankee Doodle (TPxxVIR)
Classification Resident COM and EXE infector for IBM DOS
Length of Virus Approximately 2901 bytes
Behavior Summary When an infected program is run, this virus loads into memory and infects any program run later. At 5:00 p.m. infected systems sometimes play "Yankee Doodle" through the speaker. This virus also has complex (but basically uninteresting) interactions with previous viruses in the same family, and with the Bouncing Ball virus. From your point of view, this virus is essentially identical to the Yankee Doodle-2885 virus (and some other members of this family).

The Traceback-2930 Virus

Name	Traceback-2930
Alias(es)	Traceback II
Virus Family	Traceback
Classification	Resident COM and EXE infector
Length of Virus	Approximately 2930 bytes
Behavior Summary	When an infected program is run, the virus installs itself in memory and also looks for a file to infect on the current disk. Any files executed later can also become infected. Approximately one hour after executing the first infected program, a "falling letters" display, similar to that produced by the 17xx family of viruses, will occur. At the first keystroke after the display, the screen returns to normal; this performance is repeated periodically. This virus is very similar to the 3066 virus.

The Traceback-3066 Virus

Name	Traceback-3066
Alias(es)	Traceback
Virus Family	Traceback
Classification	Resident COM and EXE infector
Length of Virus	Approximately 3066 bytes
Behavior Summary	When an infected program is run, the virus installs itself in memory and also looks for a file to infect on the current disk. Any files run later can also become infected. Approximately one hour after running the first infected program, a "falling letters" display, similar to that produced by the 17xx family of viruses, occurs. At the first keystroke after the display, the screen returns to normal. This performance is repeated periodically. This virus is very similar to the 2930 virus.

The VACSINA Virus

Name	VACSINA
Alias(es)	
Virus Family	TPxxVIR
Classification	Resident EXE-converter and COM infector for IBM DOS
Length of Virus	Approximately 1206 bytes
Behavior Summary	This virus converts EXE-formatted files to COM format, and infects COM-format files. The virus becomes resident when the first infected file is run and converts or infects any files that are run later. The system might "beep" when new files are infected.

The Vienna-Ghost Virus

Name	Vienna-Ghost
Alias(es)	Ghostballs
Virus Family	Vienna, Bouncing Ball
Classification	Non-resident COM infector / boot modifier
Length of Virus	2351 bytes

Behavior Summary This virus infects COM files exactly as the Vienna-648 virus does, except it does not do the file damage of the Vienna-648 virus. When an infected file is run, the virus (as well as spreading) writes to drive A a boot sector that resembles the Bouncing Ball/286 boot sector in all functions **except** spreading. That is, the new boot sector sometimes produces a bouncing ball on the screen after booting and is detected as infected by the Bouncing Ball virus by some detectors, but it will not spread itself to other diskettes (only COM files infected with the Ghost virus spread it).

The Vienna-Lisbon Virus

Name	Vienna-Lisbon
Alias(es)	Lisbon
Virus Family	Vienna
Classification	Non-resident COM file virus for IBM DOS
Length of Virus	648 bytes
Behavior Summary	This virus overlays some COM files with the string "@AIDS", rendering them nonfunctional.

The Vienna-648 Virus

Name Vienna-648
Alias(es) Austrian, DOS-62, DOS-68, One-In-Eight, Reboot, Unesco, Vienna
Virus Family Vienna
Classification Non-resident COM file virus for IBM DOS
Length of Virus 648 bytes
Behavior Summary When an infected program is run, this virus looks for one uninfected COM file along the DOS PATH and infects it. It overlays some COM files with code that reboots the machine.

The W13-A Virus

Name	W13-A
Alias(es)	Polish
Virus Family	W13
Classification	Non-resident COM file virus for IBM DOS
Length of Virus	534 bytes
Behavior Summary	Infected COM files infect other COM files when they are run. No other effects.

The W13-B Virus

Name	W13-B
Alias(es)	Polish
Virus Family	W13
Classification	Non-resident COM file virus for IBM DOS
Length of Virus	507 bytes
Behavior Summary	Infected COM files infect other COM files when they are run. No other effects.

The Yale Virus

Name	Yale
Alias(es)	Alameda, Merritt, Peking, Seoul, Yale Boot
Virus Family	Yale
Classification	Diskette boot infector
Length of Virus	Boot record and one additional hard disk or diskette sector
Behavior Summary	This virus has no obvious damage or symptoms; spreads when Ctrl+Alt+Del is pressed in an infected machine with an uninfected diskette in drive A.

The Yankee Doodle-2772 Virus

Name Yankee Doodle-2772
Alias(es) Yankee Doodle, 2772, TP39VIR, Yankee Doodle-B
Virus Family Yankee Doodle (TPxxVIR)
Classification Resident COM and EXE infector for IBM DOS
Length of Virus Approximately 2772 bytes
Behavior Summary When an infected program is run, the virus loads into memory and infects any program run later. At 5:00 p.m. infected systems sometimes play "Yankee Doodle" through the speaker. This virus also has complex (but basically uninteresting) interactions with previous viruses in the same family and with the Bouncing Ball virus. From your point of view, this virus is essentially identical to the Yankee Doodle-2885 (and some other members of this family).

The Yankee Doodle-2885 Virus

Name	Yankee Doodle-2885
Alias(es)	Yankee Doodle, 2885, TP44VIR
Virus Family	Yankee Doodle (TPxxVIR)
Classification	Resident COM and EXE infector for IBM DOS
Length of Virus	Approximately 2885 bytes

Behavior Summary When an infected program is run, the virus loads into memory and infects any program run later. At 5:00 p.m. infected systems sometimes play "Yankee Doodle" through the speaker. This virus also has complex (but basically uninteresting) interactions with previous viruses in the same family and with the Bouncing Ball virus. From your point of view, this virus is essentially identical to the Yankee Doodle-2772 (and some other members of this family).

The 1381 Virus

Name	1381
Alias(es)	Internal
Virus Family	
Classification	Non-resident EXE infector for IBM DOS
Length of Virus	Approximately 1381 bytes

Behavior Summary When an infected file is run, the virus looks for an uninfected file with an extension of EXE on the current disk (it looks randomly through subdirectories) and infects it. If an infected file is run more than about 90 days after it became infected, it will display random-looking characters across the screen, along with the message "INTERNAL ERROR 02CH. PLEASE CONTACT YOUR HARDWARE MANUFACTURER IMMEDIATELY ! DO NOT FORGET TO REPORT THE ERROR CODE !" The virus then removes itself from the infected file and you are returned to DOS.

The 1392 Virus

Name 1392
Alias(es) Amoeba, Khetapunk
Virus Family
Classification Resident COM and EXE infector for IBM DOS
Length of Virus Approximately 1392 bytes
Behavior Summary When an infected file is run, the virus installs itself in memory. While in memory, the virus attempts to infect files that are run, and COMMAND.COM files on any disk while a free-space check is made. The DIR command, for instance, does a free-space check. When the virus has gone about four minutes without infecting a file and the display is a CGA (in text mode), the virus talks to the CRT controller to create a 26th line on the display and writes the words "SMA KHETAPUNK - NOUVEL Band   A.M.O.E.B.A. by PrimeSoft Inc" in yellow on purple background.

The virus contains a serious bug that causes it to replicate imperfectly, and only early generations of the virus are likely to function.

The 1536 Virus

Name 1536
Alias(es) Zero Bug, Palette
Virus Family
Classification Resident COM infector for PC DOS
Length of Virus 1536 bytes
Behavior Summary This virus infects COMMAND.COM and other COM files that are copied. Under some conditions, a "face" appears on the screen, and "eats" displayed characters.

The 1575 Virus

Name	1575
Alias(es)	Green Caterpillar
Virus Family	
Classification	Resident COM and EXE infector for IBM DOS
Length of Virus	Approximately 1575 bytes

Behavior Summary When an infected file is run, it attempts to infect the COMMAND.COM file in the root directory of drive C and loads itself into memory if it is not already present. It then infects files with an extension of COM or EXE that are found by various file-search calls (a DIR, for instance, often causes files found to be infected). At times, the virus displays a small horizontal green caterpillar running across your color display, moving characters around on the screen and changing their color.

The 1701 Virus

Name 1701
Alias(es) 170x, 17xx, Austrian 2, Autumn, Blackjack, Cascade, Fall, Falling Tears
Virus Family 17xx
Classification Resident COM infector for IBM DOS
Length of Virus 1701 bytes
Behavior Summary When an infected program is run, the virus loads into memory and infects COM-formatted files run later. The virus occasionally causes letters on the screen to fall into a pile at the bottom of the display screen, while causing "clicks" on the speaker. Due to complex date interactions, it is possible to have an active 1701 infection without this symptom ever appearing.

The 1701-NoDate Virus

Name	1701-NoDate
Alias(es)	
Virus Family	17xx
Classification	Resident COM infector for IBM DOS
Length of Virus	1701 bytes
Behavior Summary	This virus spreads between COM files in IBM DOS. Occasionally the virus causes letters on the screen to fall into a pile at the bottom of the screen. It is a minor variant of the 1701 virus.

The 1704 Virus

Name	1704
Alias(es)	170x, 17xx, Austrian 2, Autumn, Blackjack, Fall, Second Austrian
Virus Family	17xx
Classification	Resident COM infector for IBM DOS
Length of Virus	1704 bytes
Behavior Summary	This virus spreads among COM files in IBM DOS. Occasionally the virus causes letters on the screen to fall into a pile at the bottom.

The 1704-B Virus

Name	1704-B
Alias(es)	170x, 17xx, Cascade-B
Virus Family	17xx
Classification	Resident COM infector for IBM DOS
Length of Virus	1704 bytes
Behavior Summary	This virus spreads among COM files in IBM DOS. Occasionally the virus causes letters on the screen to fall into a pile at the bottom.

The 1704-C Virus

Name	1704-C
Alias(es)	170x, 17xx
Virus Family	17xx
Classification	Resident COM infector for IBM DOS
Length of Virus	1704 bytes
Behavior Summary	This virus spreads among COM files in IBM DOS. Occasionally this virus causes letters on the screen to fall into a pile at the bottom.

The 1704-Format Virus

Name 1704-Format
Alias(es) 170x, 17xx
Virus Family 17xx
Classification Resident COM infector for IBM DOS
Length of Virus 1704 bytes
Behavior Summary This virus spreads among COM files in IBM DOS. Under some conditions, the virus renders data on drive C unreadable.

The 1704-Y Virus

Name	1704-Y
Alias(es)	170x, 17xx
Virus Family	17xx
Classification	Resident COM infector for IBM DOS
Length of Virus	1704 bytes
Behavior Summary	This virus spreads among COM files in IBM DOS. Occasionally this virus causes letters on the screen to fall into a pile at the bottom. Infected programs often malfunction. This is a damaged variant of the 1704 virus.

The 1813 Virus

Name 1813
Alias(es) Black Friday, Black Hole, Hebrew University, Israeli, Jerusalem, JV, Morbus Waiblingen, PLO, Russian, sUMsDos
Virus Family 1813
Classification Resident COM and EXE file virus for IBM DOS
Length of Virus 1813 bytes in infected COM files; some additional padding bytes in infected EXE files.
Behavior Summary When an infected program is run, the virus loads into memory and infects any program run later. Because of a bug in the virus, EXE-formatted files are infected each time they are run. Frequently used files eventually become too large to run. Because of another bug, some files (including OS/2 and Windows EXE files and very large COM files) do not run correctly after being infected. The virus intentionaly causes slowing down of the machine at intervals. Also, causes the appearance of "black boxes" on the display, and erases any file executed on any Friday the 13th.

The 1813-00 Virus

Name 1813-00
Alias(es)
Virus Family 1813
Classification Resident COM and EXE infector for IBM DOS
Length of Virus 1813 bytes in infected COM files; some additional padding bytes in infected EXE files.
Behavior Summary This virus is a "mutation" (either accidental or intentional) of the standard 1813 virus. One byte of the virus has been changed to a zero. The main effect is if an uninfected program is run from a write-protected diskette while the virus is active in memory, the program often does not run at all and simply exits back to the DOS command prompt. With this exception, the virus is almost identical to the standard 1813 virus.

The 1813-ANARKIA Virus

Name 1813-ANARKIA
Alias(es)
Virus Family 1813
Classification Resident COM and EXE file virus for IBM DOS
Length of Virus 1813 bytes in infected COM files; some additional padding bytes in infected EXE files.
Behavior Summary This virus erases files run on Friday the 13th and causes some odd system behavior. This virus is a slight variant of the 1813 virus. It never causes the 1813 virus's "black box," and has a more drastic system slowdown at times.

The 1813-Discom Virus

Name 1813-Discom
Alias(es) Discom
Virus Family 1813
Classification Resident COM and EXE infector for IBM DOS
Length of Virus 2053 bytes in infected COM files; some additional padding bytes in infected EXE files.
Behavior Summary Like the 1813 virus, the Discom virus loads into memory and infects COM and EXE files that are later run. But, unlike the 1813, it does not infect EXE files multiple times and will not infect files with names ending in the letters "acad". Rather than erasing files run on Friday the 13th, the Discom virus has a number of side effects, such as slowing down the system, sending random data out the serial I/O ports, and sometimes overlaying data on the hard drive.

The 1813-Not-13 Virus

Name 1813-Not-13

Alias(es) Payday

Virus Family 1813

Classification Resident COM and EXE file virus for IBM DOS

Length of Virus 1813 bytes in infected COM files; some additional padding bytes in infected EXE files.

Behavior Summary This virus erases files run on Fridays that are not the 13th of the month and causes some odd system behavior. This virus is an almost-identical variant of the 1813 virus.

The 1813-Swiss Virus

Name 1813-Swiss
Alias(es)
Virus Family 1813
Classification Resident COM and EXE file virus for IBM DOS
Length of Virus 1813 bytes in infected COM files; some additional padding bytes in infected EXE files.
Behavior Summary This virus erases files run on Friday the 13th and causes some odd system behavior. This virus is a functionally identical code variant of the 1813 virus.

The 1813-Tuesday-the-13th Virus

Name 1813-Tuesday-the-13th
Alias(es)
Virus Family 1813
Classification Resident COM and EXE file virus for IBM DOS
Length of Virus 1813 bytes in infected COM files; some additional padding bytes in infected EXE files.
Behavior Summary This virus erases files executed on Tuesdays that are also the 13th of the month and causes some odd system behavior. It is an almost identical variant of the 1813 virus.

The 2086 Virus

Name 2086
Alias(es) Fu Manchu
Virus Family 1813
Classification Resident COM and EXE file virus for IBM DOS
Length of Virus 2086 bytes in infected COM files; some additional padding bytes in infected EXE files. (More precisely, 2080 bytes of code and 6 bytes of virus self-recognition string in COM files, and 0-15 bytes of padding followed by 2080 bytes of code in EXE files.)
Behavior Summary This virus hooks the keyboard interrupts, waits for any of the names "Fu Manchu, Reagan, Thatcher, Botha, or Waldeim" to be typed in upper case or lower case letters followed by a space, and adds its own remarks about them in the keyboard buffer so they are entered as the rest of the text. Also this virus slowly displays a message when the system is restarted by pressing Ctrl+Alt+Del.

The 4096 Virus

Name	4096
Alias(es)	Stealth, Century
Virus Family	
Classification	Resident EXE and COM infector for IBM DOS
Length of Virus	4096 bytes

Behavior Summary When an infected program is run, the virus becomes resident in memory and infects any files run and any executable files opened and closed later. If the date is between September 22 and December 31 of any year, the virus will generally hang the machine (due to bugs in code that seem to be intended to overwrite the boot record with a program to display the message "Frodo Lives" when the machine boots).

The 555 Virus

Name 555
Alias(es) QUIT1992
Virus Family 555
Classification Resident COM and EXE infector for IBM DOS
Length of Virus 555 bytes in infected COM files; some additional padding bytes in infected EXE files.
Behavior Summary When an infected file is run, the virus loads into memory and infects EXE and COM files that are later run. If the year is 1992 or greater when an infected file is executed, the virus will install itself and exit immediately to DOS, without running the original victim program.

The 555-B Virus

Name 555-B
Alias(es) QUIT1992
Virus Family 555
Classification Resident COM and EXE infector for IBM DOS
Length of Virus 555 bytes in infected COM files; some additional padding bytes in infected EXE files.
Behavior Summary When an infected file is run, the virus loads into memory and infects EXE and COM files that are later run. If the year is 1992 or later when an infected file is run, the virus will install itself and will exit immediately to DOS, without running the original program. This virus is almost identical to the 555 virus.