

Computer Viruses

Microcomputer Viruses

Getting Started Guide



FAA Operational Support

AOS-500, FAA William J. Hughes Technical Center
Atlantic City International Airport, NJ 08405
Main & Tech Support: (609)485-HELP
Fax: (609)485-4235

Table of Contents

| | |
|--|-------------|
| 1. COMPUTER VIRUSES..... | 1-3 |
| INTRODUCTION..... | 1-3 |
| RIT SYSTEM VIRUS PROTECTION..... | 1-3 |
| <i>AOS Intranet Web Site</i> | <i>1-3</i> |
| WHAT IS A COMPUTER VIRUS? | 1-4 |
| HOW DOES A COMPUTER VIRUS WORK?..... | 1-4 |
| SPREADING THE “INFECTION” | 1-4 |
| WHAT DO VIRUSES DO? | 1-4 |
| WHAT VIRUSES DON’T DO | 1-5 |
| TYPES OF VIRUSES | 1-5 |
| <i>Program Viruses</i> | <i>1-6</i> |
| <i>Boot Viruses</i> | <i>1-6</i> |
| <i>Companion Viruses</i> | <i>1-7</i> |
| <i>Armored Viruses.....</i> | <i>1-7</i> |
| <i>Multipartite Viruses.....</i> | <i>1-7</i> |
| <i>Stealth Viruses.....</i> | <i>1-7</i> |
| <i>Polymorphic Viruses</i> | <i>1-7</i> |
| <i>Macro Viruses</i> | <i>1-8</i> |
| <i>Are there CMOS viruses?.....</i> | <i>1-8</i> |
| <i>Are there BIOS viruses?.....</i> | <i>1-9</i> |
| THE VIRUS INFECTION CYCLE | 1-9 |
| <i>Infection Stage.....</i> | <i>1-9</i> |
| <i>Detection Stage</i> | <i>1-10</i> |
| <i>Recovery Stage.....</i> | <i>1-10</i> |
| HOW DOES ANTI-VIRUS SOFTWARE WORK? | 1-10 |
| HOW CAN I AVOID INFECTION? | 1-10 |
| <i>CMOS Settings</i> | <i>1-11</i> |
| DO I HAVE A VIRUS, AND HOW DO I KNOW?..... | 1-11 |
| I’VE GOT A VIRUS! | 1-12 |
| <i>I Have A Virus Problem - What Do I Do?</i> | <i>1-12</i> |
| <i>False Alarm Indicators</i> | <i>1-12</i> |
| <i>Virus Infection Indicators</i> | <i>1-13</i> |
| <i>Tell You Nothing Indicators</i> | <i>1-13</i> |
| <i>Removing viruses</i> | <i>1-13</i> |
| VIRUS PREVENTION..... | 1-15 |
| <i>Hints and Tips</i> | <i>1-15</i> |
| WHAT SHOULD BE ON A (CLEAN) BOOT DISK? | 1-15 |
| <i>Boot Floppy Files.....</i> | <i>1-16</i> |
| <i>What Other Tools Might I Need?</i> | <i>1-17</i> |
| <i>How Do I Know I Have A Clean Boot Disk?</i> | <i>1-18</i> |
| WHAT ARE RESCUE DISKS?..... | 1-19 |
| <i>Maintaining A Rescue Disk.....</i> | <i>1-19</i> |
| <i>Why Create A Rescue Disk?.....</i> | <i>1-19</i> |

| | |
|---|------|
| <i>When To Update The Rescue Disk</i> | 1-20 |
| HOW TO CREATE A RESCUE DISK | 1-20 |
| <i>Creating Rescue Disks</i> | 1-20 |
| <i>Steps To Create Or Update NAV Rescue Disk #1</i> | 1-20 |
| <i>Steps To Create Or Update NAV Rescue Disk #2</i> | 1-21 |
| UPDATING VIRUS DEFINITIONS | 1-21 |
| <i>Update Virus Definitions Automatically</i> | 1-22 |
| <i>Update The Virus Definitions Files Yourself</i> | 1-22 |

1. Computer Viruses

RIT Systems affected: All fielded RIT and E-RIT Systems

Introduction

Normal Radar Intelligent Tool (RIT) operations requires frequent passing of files and disks between people and computers. The likelihood that a RIT System will be infected by a computer virus increases with each occurrence.

A computer virus may degrade the operating performance of a PC or may corrupt and destroy data located on the PC including the data that may be passed into NAS. A computer virus may corrupt or invalidate an operational radar certification procedure or skew the performance data analysis. Data that may not be able to be replaced. Protection against computer virus infections is a high priority.

Recommendation: Institution of computer virus protection procedures are strongly recommended.

RIT System Virus Protection

All RIT/E-RIT Systems are licensed to use Symantec's Norton AntiVirus (NAV) software utility. NAV v3.0 has been installed on the new release of the RIT System hard drive backup image distributed on the RIT System CD-ROM disk. RIT users are encourage to restore the new backup hard drive image (see Restore Hard Disk chapter). Users can make NAV v3.0 installation disks from the RIT System CD-ROM disk (see Making Install Disks chapter). RIT users are required to have blank diskettes available.

Free monthly virus definition updates for NAV v3.0 are available from:

Symantec's Internet World Wide Web site: <http://www.symantec.com/>.

AOS Intranet Web site: <http://www.aos.tc.faa.gov/AOS270/>.

AOS Help Line (609) 485-HELP.

AOS Intranet Web Site

AOS maintains an FAA Intranet World Wide Web (WWW) site.

<http://www.aos.tc.faa.gov/>

For radar analysis tools go to <http://www.aos.tc.faa.gov/AOS270/>.

You will be able to view radar analysis information on-line and download program updates and new programs.

What is a computer virus?

A computer virus is simply, a specially designed computer program written with the intention to alter the way your computer operates without your permission or knowledge.

Computer viruses have become a serious problem. The lack of security on PC machines, including RIT Systems, enables viruses to spread easily, even infecting the operating system.

How does a computer virus work?

A computer virus (by analogy with biological viruses) is, a computer program, written by an ill-intentioned programmer, that searches out other programs and "infects" them by embedding a copy of itself in them. The infected computer programs become "Trojan horses" or malicious, security-breaking programs that disguise themselves as something harmless, such as a directory lister or other familiar utility program.

When "infected" programs are executed, the embedded virus is executed (activated) too, thus propagating the "infection". The user is normally unaware that any malicious, covert activity is going on.

Note: A computer virus, like biological viruses, "lives" only to replicate itself.

Spreading the Infection

A computer virus cannot infect other computers without assistance. In other words, a computer virus is inactive until you execute an infected program, or start (boot) your computer from an infected disk or access an infected disk.

Caution ! A computer virus is propagated by carriers, normally humans, exchanging software with friends and coworkers.

Typically, computer viruses spread when you execute an infected program file (files with a .COM, .EXE, .OVL, .DRV, .SYS, or .BIN file extension). For example, if a word processing program is infected with a virus, the virus activates when you run (double-click the icon) the application program. Once a virus is in memory, it usually infects any application program you run thereafter, including network programs (if you have write access to your network directories).

What do viruses do?

Viruses do not infect or damage hardware, such as keyboards or monitors. Though you may experience strange behaviors such as screen distortion or characters not appearing when typed, a virus has, in fact, merely affected the programs that control the display or keyboard. Your hard disks and floppy disks have not been physically damaged, only the electronic data that was stored on them was damaged (corrupted).

Most viruses stay active in your computer memory (RAM) until you power off your computer. Powering off your computer removes the virus from memory only and does not remove the virus from the infected files or disks. If the virus resides in a program file, such as a word processing application or the keyboard driver program, the virus will activate and load into memory again the next time the program is run. If a virus resides in a disk boot record or a master boot record, such as on your hard disk or a floppy disk, the virus will activate the next time you boot your computer or access that disk, even if it has laid dormant for many months.

A virus may do nothing but propagate itself and then allow the “host” program to run normally. Usually, however, after propagating silently for a while, the virus starts doing things like writing “cute” messages on the screen or playing strange tricks with the display. Many nasty viruses, written by particularly antisocial programmers, do irreversible damage, like deleting all the user's files from the hard disk. Most viruses are not designed to do serious damage; they simply replicate or display messages.

Even though you may never have experienced a computer virus, you’ve probably heard of some of the more famous ones. For example, the Michelangelo virus quietly spreads until March 6th when it overwrites the information on your hard disk with random characters. The Keypress virus makes keystrokes repeat on the screen, such as, you might press the ‘ A ’ key once, but “A A A A A” appears on your screen.

What viruses don t do

Computer viruses can not infect write-protected disks. Viruses usually do not infect data files nor do they infect compressed files such as .ZIP files. However, programs contained within a compressed file could have been infected prior to being compressed.

Viruses do not infect computer hardware, such as keyboards or monitors; they usually infect only executable program files.

Warning ! Computer viruses do not necessarily let you know they are present - even after they do something destructive.

Types of Viruses

Computer viruses are classified by their targets, the items they infect:

- **Program viruses:** These viruses infect executable files such as word processing, spreadsheet, computer game, or operating system programs.
- **Boot viruses:** Some viruses can “infect” disks by attaching themselves to special programs in areas of your disks called boot records and master boot records. These areas contain the programs your computer uses to start up.

- **Marco viruses:** In many word processing and spreadsheet applications, you can record a macro that stores a series of actions. Later, you can run the macro and automatically repeat the same actions. Macro viruses infect data files with macro capabilities. For example Microsoft Word document and template files are susceptible to macro virus attacks.

There are two main types of computer viruses: program viruses and boot viruses. Program viruses infect programs that run on your computer, and boot viruses infect the boot records and master boot records on disks (hard disks and floppy disks).

Some viruses (called multipartite viruses) fall into both categories. They have the ability to infect program files, boot records, and master boot records. In addition, particular viruses in these categories may also be characterized as stealth or polymorphic viruses. They each have a unique way of making detection more difficult.

Program Viruses

A program virus attacks executable program files, which often have one of these file extensions: .COM, .EXE, .OVL, .DRV, .SYS, or .BIN.

Many program viruses remain active in your computer's memory (RAM) after an infected program is executed until you turn off your computer. While in memory, they continue to infect other programs and can interfere with normal operations.

Examples of program viruses: Sunday and Cascade

Boot Viruses

Boot viruses attack the boot records and master boot records on disks, floppy and hard disks. Boot records and master boot records contain the information your computer requires to start (boot up). You boot your computer either by powering it on, known as a "cold boot" or by pressing the <CTRL> + <ALT> + keyboard key combination when the computer is already on, known as a "warm boot".

When a computer boots up, it runs specific boot record programs to ready itself for work. These boot record programs are infected by boot viruses. All disks, floppy disks and hard disks have boot records. Floppy disks have boot records and hard disks have boot records or master boot records.

The disk does not have to be bootable to be infected by a boot virus. Data disks can contain boot viruses too. Data disks are non-bootable floppy disks or removable media disks or the second installed hard disk.

A boot virus activates when your computer either attempts to start up from the infected disk or access data from the infected disk. All boot viruses remain active in memory while your computer is on. While in memory they continue to spread by infecting floppy disks your computer accesses. A common scenario is to boot (or reboot) your computer when there is an infected floppy disk in the A : drive. When your computer attempts to read the floppy disk, the virus loads into memory and then infects your hard disk's boot record. Once a boot virus is in memory, it can spread covertly to every disk you access. Boot viruses never spread across a network, nor can they be downloaded from a bulletin board.

Examples of boot viruses: Disk Killer, Michelangelo, Ripper, and Stoned

Companion Viruses

Companion (or spawning) viruses spread via a file which runs prior the original file the user intended to run. For instance, the file MYAPP.EXE might be infected by creating a file called MYAPP.COM. Because of the way DOS works, when the user types MYAPP at the C : \ > prompt, MYAPP.COM is run instead of the program MYAPP.EXE. DOS was designed to execute .COM files before .EXE files and .EXE programs are executed before .bat files. MYAPP.COM runs its infective routine, then quietly executes MYAPP.EXE.

Note: This is not the only type of companion (or 'spawning') virus.

Armored Viruses

Armored viruses are specifically written to make it difficult for an anti-virus researcher to find out how they work and what they do.

Multipartite Viruses

Multipartite viruses are both program viruses and boot viruses. For example, if you run a word processing application infected with the Tequila virus, the virus activates and infects the master boot record on your hard disk. Then, the next time you boot your computer, the Tequila virus activates again and starts infecting every program you run.

Examples of multipartite viruses: Tequila, Invader and Flip

Stealth Viruses

Stealth viruses actively seek to conceal themselves from attempts to analyze or remove them. Stealth techniques include redirecting disk reads (full-stealth viruses) and altering disk directory data (size-stealth viruses).

The Whale virus infects .EXE program files and alters the directory entries on infected file when other programs attempt to read them. For example, the Whale virus adds 9216 bytes to an infected file; the virus then subtracts the same number of bytes (9216) from the file size given in the directory entry to give the impression that the file's size has not changed. (Changes in file size are an indication that a virus might be present).

Examples of stealth viruses: Whale, Frodo and Joshi

Polymorphic Viruses

Polymorphic viruses are mutating viruses that change their telltale code segments so that they "look" different from one infected file to another. This dynamic pattern of alteration is an effort to conceal itself from unwary anti-virus programs.

Included among polymorphic viruses are MtE (Mutation Engine) assisted viruses that use an encryption technique called the mutation engine. The mutation engine is not a virus itself, but a method of creating complex polymorphic viruses.

Example of a polymorphic virus: Involuntary

Macro Viruses

Macro viruses are the latest development in the battle against computer viruses. First encountered in the autumn of 1995 they have quickly caught the imagination of the press and virus-author alike. Their introduction into the virus world has caused a stir because they have broken some of the established "rules":

- They are the first ever viruses to infect documents rather than executable files. The first macro viruses seen infected Microsoft Word for Windows documents. In January 1996 the first AmiPro macro virus (APM Green Stripe) appeared. It should be remembered that other word processors could be at risk in the future. XM.Laroux, which appeared in July 1996, is the first working macro virus which infects Microsoft Excel for Windows spreadsheets.
- They are the first ever multi-platform viruses - not just capable of infecting PC systems, but Macintosh as well

Macro viruses work because the files to which they are attached are not 'pure' data files. In general, file viruses don't infect data files. However, data files can contain embedded executable code such as macros, which may be used by virus or Trojans writers.

Macro viruses are limited to the specific applications for which they were written. One, now widespread virus, infects macros attached to Microsoft Word 6.0 for Windows, Microsoft Word 6.0.1 for Macintosh, Microsoft Word 6.0 for Windows NT, and Microsoft Word for Windows 95 documents. This macro virus, named "Concept", is specific to Microsoft Word 6/WordBasic and Excel, however, many applications, not all of them Windows applications, also have potentially damaging and infective macro capabilities.

What makes such a virus possible is that the macros are created by WordBASIC, a programmatic language which links features used in Word to macros, and even allows DOS commands to be run. Surprisingly, macro viruses are written in macro languages.

The Concept virus has no destructive payload; it merely spreads, after a document containing the virus is opened, copying itself to other documents as they are saved, without affecting the contents of documents. However, other macro viruses have been discovered, and some of them contain destructive routines.

Are there CMOS viruses?

Although a virus can write to and corrupt a PC's CMOS memory, it can NOT "hide" there. The CMOS memory used for system information and is backed up by battery power is not "addressable" and requires Input/Output (I/O) instructions to be usable.

Data stored there is not loaded from there and executed, so virus code written to CMOS memory would still need to infect an executable program in order to load and execute whatever it wrote.

A virus could use CMOS memory to store part of its code, and some tamper with the CMOS Setup's values. However, executable code stored there must first be first moved to DOS memory in order to be executed. Therefore, a virus can NOT spread from, or be hidden in CMOS memory.

Are there BIOS viruses?

There are reports of a trojanized AMI BIOS - this is not a virus, but a 'joke' program which does not replicate. The malicious program is not on the disk, nor in CMOS, but was directly coded into the BIOS ROM (Basic Input Output System Read-Only Memory) chip located on the system board by a rogue programmer at American Megatrends Inc., the manufacturer.

If the date is the 13th of November, it stops the bootup process and plays 'Happy Birthday' through the PC speaker. In this case, the only cure is a new BIOS (or motherboard). The "infected" chip run was BIOS version M82C498 Evaluation BIOS version 1.55 of 04-04-93.

The virus infection cycle

There are three stages on the life of computer viruses: infection, detection, and recovery.

| | | |
|------------------------------|--------------------|---|
| VIRUS INFECTION STAGE | Source | <ul style="list-style-type: none"> • Reused floppy diskettes from unknown or unsuspecting sources • Diskettes from home, school or work • Diskettes borrowed from friends • Software bargains (from non-reputable dealers) • Re-shrink-wrapped or opened software • Pirated software • Preformatted floppy diskettes • Files downloaded from the Internet |
| | Infection | <ul style="list-style-type: none"> • Boot from an infected diskette • Reboot with an infected diskette left in drive • Run an infected program |
| VIRUS DETECTION STAGE | Spread | <ul style="list-style-type: none"> • Share diskettes or infected programs/files • Log on to network |
| | Observation | <ul style="list-style-type: none"> • Strange system behavior • Files missing or programs not working |
| VIRUS RECOVERY STAGE | Utility | <ul style="list-style-type: none"> • Virus detected by anti-virus software |
| | Cleanup | <ul style="list-style-type: none"> • Reinstall programs from master (write protected) diskettes • Repair files with anti-virus software • Restore from uninfected backup |
| | Follow-up | <ul style="list-style-type: none"> • Rescan all files to find source of infection • Scan all floppy diskettes to find source of infection • Discard any backups that may be infected • Increase virus protection for a while |

TABLE 1. -1: VIRUS INFECTION CYCLE

Infection Stage

In the infection stage, a virus infects a file in your computer.

Detection Stage

In the detection stage, the virus is identified and isolated.

Recovery Stage

In the recovery stage, the virus is eliminated. Unless the virus is eliminated, it continues to infect other files and possibly damage data on your disks.

How Does Anti-Virus Software Work?

- Scanner (conventional scanner, command-line scanner, on-demand scanner) - a program that looks for known viruses by checking for recognizable patterns ('scan strings', 'search strings', 'signatures').
- TSR scanner - a TSR (memory-resident program) that checks for viruses while other programs are running. It may have some of the characteristics of a monitor and/or behavior blocker.
- VxD scanner - a scanner that works under Windows or perhaps under Win 95, or both which checks for viruses continuously while you work.
- Heuristic scanners - scanners that inspect executable files for code using operations that might denote an unknown virus.
- Monitor/Behavior Blocker - a TSR that monitors programs while they are running for behavior which might denote a virus.
- Change Detectors/Checksummers/Integrity Checkers - programs that keep a database of the characteristics of all executable files on a system and check for changes which might signify an attack by an unknown virus.
- Cryptographic Checksummers use an encryption algorithm to lessen the risk of being fooled by a virus which targets that particular checksummer.

How Can I Avoid Infection?

There is no way to guarantee that you will avoid infection. However, the potential damage can be minimized by taking the following precautions:

- make sure you have a clean boot disk - test with whatever (up-to-date!) anti-virus software you can get hold of and make sure it is (and stays) write-protected. Boot from it and make a couple of copies.
- use reputable, up-to-date and properly-installed anti-virus software regularly. Not only does it encourage the writer and make you feel virtuous, it means you can legitimately ask for technical support in a crisis.
- do some reading. If you're a home user, you may well get an infection sooner or later. If you're a business user, it'll be sooner. Either way you'll benefit from a little background.
- always run a memory-resident scanner to monitor disk access and executable files before they're run.

- if you run Windows, a reputable anti-virus package which includes DOS and Windows components is likely to offer better protection than a DOS only package. If you run Windows 95, you need a proper Win95 32-bit package for full protection.
- make sure your home system is protected, as well as your work PC.
- check all new systems and all floppy disks when they're brought in (from any source) with a good virus-scanning program.
- acquire software from reputable sources: 2nd-hand software is frequently unchecked and sometimes infected. Bear in mind that shrink-wrapped software isn't necessarily unused. In any case, reputable firms have, unknowingly, shipped viruses.
- once formatted, keep all floppies write-disabled (write protected) except when you need to write a file to them: then write-disable them again.
- make sure your data is backed up regularly and that the procedures for restoring archived data work properly.
- scan all pre-formatted diskettes before use.
- get to know all the components of the package you're using and consider which bits to use and how best to use them. Different packages have different strengths: diversifying and mixing and matching can, if carefully and properly done, be a good anti-virus strategy, especially in a corporate environment.
- if your PC can be prevented with a CMOS setting from booting with a disk in drive A, do it (and re-enable floppy booting temporarily when you need to clean-boot).

CMOS Settings

Some CMOSes come with special anti-virus settings. These are normally vague about what they do but typically they write-protect your hard disk's boot sector and partition sector (MBR). This can be some use against boot sector viruses but may false alarm when you upgrade your operating system.

One sensible setting to make (if your CMOS allows) is to adjust the boot sequence of your PC. Changing the default boot-up drive order from A : then C : to C : will mean that the PC will attempt to boot from drive C : even if a floppy disk has been left in drive A : . This way boot sector virus infection can often be avoided. Remember to set your CMOS back temporarily if you ever do want to boot clean from floppy (for example, when running a cryptographical checksummer after a cold boot).

Do I Have A Virus, And How Do I Know?

Almost anything odd a computer may do, is (and has been) blamed on a computer "virus," especially if no other explanation can readily be found. In most cases, when an anti-virus program is then run, no virus is found.

A computer virus can cause unusual screen displays, or messages - but most don't do that. A virus may slow the operation of the computer - but many times that

doesn't happen. Even longer disk activity, or strange hardware behavior can be caused by legitimate software, harmless "prank" programs, or by hardware faults. A virus may cause a drive to be accessed unexpectedly (and the drive light to go on) - but legitimate programs can do that also.

One usually reliable indicator of a virus infection is a change in the length of executable (*.COM, *.EXE) files, a change in their content, or a change in their file date/time in the Directory listing. But some viruses don't infect files, and some of those which do can avoid showing changes they've made to files, especially if they're active in memory (RAM).

Suggestion: Ensure that all people in your office and anyone else at risk are aware of the situation.

Another common indication of a virus infection is a change to interrupt vectors or the reassignment of system resources. Unaccounted use of memory or a reduction in the amount normally shown for the system may be significant.

In short, observing "something funny" and blaming it on a computer virus is less productive than scanning regularly for potential viruses, and not scanning, because "everything is running OK" is equally inadvisable.

I've Got A Virus!

The following guidelines will be of assistance. However, read the rest of this document before acting.

Note: If you believe you may have a virus infection, *stay calm*.

Once detected, a virus will rarely cause (further) damage, but a panicked action might. Bear in mind that not every one who thinks s/he has a virus actually does (and a well-documented, treatable virus might be preferable to some problems!).

I Have A Virus Problem - What Do I Do?

So you think you've got a virus. Maybe you have, maybe you haven't. This section will help you decide. A lot of people have problems with their computers, and the problem can be hardware, software, user error, and many other things.

Warning ! Rule number one - *Don't Panic*.

False Alarm Indicators

First of all, why do you think you have a virus? Is it because an anti-virus package told you so? Like other software, anti-virus software is not infallible, and some anti-virus packages give many false alarms. Here are some indicators that it might be a false alarm:

- Only one file is infected on your hard disk.

- The virus being reported is one of the several thousand that are not known to be in the wild
- The anti-virus package doesn't name the virus that it thinks you have
- Read the technical note on false alarms.

Virus Infection Indicators

Here are some indicators that it might really be a virus. They are just indicators; none of them say that you definitely have a virus:

- According to an anti-virus package, several files on the computer are infected, all with the same virus
- It is a virus that is known to be in free distribution among the general public (“in the wild”).
- More than one anti-virus package agrees that you have a virus.
- Several .COM and/or .EXE files on your computer are all larger than they used to be, by about the same amount.
- Windows refuses to use 32 bit disk access, or 32 bit file access.
- If the anti-virus utility says that it has identified the virus, then it means that it has not just found a byte-signature, it means that it has checksummed all the constant virus bytes, and they match the checksum in it's database. So it's very unlikely to be a false alarm.

Tell You Nothing Indicators

Here are some indicators that tell you nothing about the likelihood that you have a virus (included here because many people think that they are infected):

- Your hard disk doesn't work any more
- You're getting unusual graphics on your screen
- Your hard disk light seems to come on for no particular reason
- You just ran some downloaded software

Caution ! Reformatting your hard disk is almost certainly unnecessary and very probably won't kill the virus.

If you've been told you have something exotic, consider the possibility of a false alarm and check with a different package.

Removing viruses

Note: Remember, that the time to really worry about computer virus infections is *before* your computer gets one!

It is always better from a security point of view to replace infected files with clean, uninfected copies. However, in some circumstances this is not convenient. For example, if an entire network were infected with a fast-infecting file virus then it may be a lot quicker to run a quick repair with a reliable anti-virus product than to find clean, backup copies of the files. It should also be realized that clean backups are not available. If a site has been hit by Nomenklatura, for example, it may take a long time before it is realized that you have been infected. By that time the data in backups have been seriously compromised.

There are virtually no circumstances under which you should need to reformat a hard disk, however: in general, this is an attempt to treat the symptom instead of the cause. Likewise re-partitioning with FDISK.

If you use a generic low-level format program, i.e., one which isn't specifically for the make and model of drive you actually own, you stand a good chance of trashing the drive more thoroughly than any virus yet discovered.

Note: Users should ensure that they have backups of important data files.

If you are sure that you are infected with a virus follow these guidelines listed below as far as is practicable and applicable.

- Report the virus infection to local authorities.
- Report the virus infection to AOS: (609) 485-HELP.
- Do not attempt to continue to work with an infected system, or let other people do so.
- If you have a good anti-virus package, use it. Better still, use more than one. If there's a problem with the package, use the publisher's tech support and/or try an alternative package. If you don't have a package, get one (see section on sources below). If you're using Microsoft's package (MSAV) get something less out-of-date.
- Generally, it's considered preferable to power off an infected system until a knowledgeable person can deal with it: do not allow other people to use the infected PC in the meantime (put a sign on the PC). If possible, close down applications, Windows etc. properly and allow any caches/buffers to flush, rather than just hit the power switch.
- If you have the means of checking other machines for infection, you should do so and take the appropriate steps if an infection is found.
- If you are unable to check other machines, assume that all machines are infected and take all possible steps to avoid spreading infection any further.
- If there are still uninfected systems in the locality, don't use floppy disks on them [except known clean write-protected DOS boot floppies]
- Users of infected machines should not under any circumstances trade disks with others until their systems and disks are cleaned.
- No files should be exchanged between machines by any means until it's established that this can be done safely.
- Get all floppy disks together for checking and check every one. This includes write-protected floppies and program master disks. Check all backups too (on tape or file servers as well as on floppy).

Recommendation: Ensure that all people in your office and anyone else at risk are aware of the situation. You should ensure that the network administrator or other responsible and knowledgeable individual in your organization is fully aware of the situation.

- If the infected system is connected to a local area network (LAN), such as Novell Netware, Microsoft Network or Appleshare etc., it should be logged off all network/remote machines unless someone knowledgeable says different. If you're not sure how to do this, contact the network administrator.

Virus Prevention

All RIT (and E-RIT) Systems should have a anti-virus protection utility installed and activated to detect potential infections. Norton Anti-Virus v3.0 is available for all RIT Systems.

Hints and Tips

If you follow a few simple guidelines, the risk of a virus attack can be reduced to virtually zero.

- Never use a 'foreign' floppy disk or CD ROM without first scanning for viruses.
- When downloading from the Internet or bulletin boards, always scan the files before running them.
- Never boot your PC from a floppy disk unless you are certain that it is clean and free from viruses.
- Use the write protect tab to prevent viruses copying themselves onto floppy disks when you use them.
- Always use licensed copies of software obtained from a reputable source.
- Use password security on your PC (if available) to prevent unauthorized copying of files in your absence.
- Make regular backup copies of all your work and system configurations and store them securely.
- Install and make regular use a regular anti-virus software such as Norton's Anti-Virus.
- Make sure that it is regularly updated to take account of new viruses and variants. NAV virus definition updates are available from AOS: (609) 485-HELP.

What should be on a (clean) boot disk?

A boot floppy is one which contains the basic operating system, so that if the hard disk becomes inaccessible, you can still boot the machine to attempt some repairs.

Remember ! All formatted floppies contain a boot sector, but only floppies which contain the necessary system files can be used as boot floppies.

A clean boot disk is one which is known not to be virus-infected. It's best to use a clean boot disk before routine scans of your hard disk(s). Some anti-virus packages will refuse to run if there is a virus in memory. It is usually better and sometimes mandatory to disinfect a system without the virus in memory, and an undetected file virus may actually spread faster during a scan, since scanners normally open all executable files in all directories.

To make an emergency bootable floppy disk, put a disk in drive A and type:

```
FORMAT A: /S
```

Be careful to avoid 'cross-formatting', i.e. formatting a double-density disk as high-density or vice versa, if your system allows this. (You should avoid this all the time, not just when creating a boot disk.)

You can also make a pre-formatted floppy (data disk) into a boot disk by transferring the system boot files to the floppy by typing:

```
SYS A:
```

Boot Floppy Files

You may be aware that if there is a problem with your boot sequence, you can boot from the hard disk on a DOS 6/7/Win95 system while bypassing AUTOEXEC.BAT and CONFIG.SYS. This is not as good as a clean floppy boot: it won't help at all if you have a boot sector/partition sector infector, or if any or all of the basic operating system files have been infected by a file virus.

The boot disk should have been created with the same version of DOS as you have on your hard disk (ideally). It should also include any drivers necessary to access your hard disk and other devices (SCSI drivers). If, for some reason, you can't obtain a clean boot disk with the same version of DOS, you can often get away with booting from a clean disk using a different version, though: there are viruses which exploit a bug in recent versions of MS-DOS which will prevent a clean boot from DOS v4.0 and up (i.e., DOS v5.0 and v6.0).

Remember ! If you do use a different version of DOS on the clean boot disk from, remember that you won't be able to use many of the standard DOS system utilities on the hard disk. When you try to run DOS utilities with a different DOS version, DOS will simply return a message like: 'WRONG DOS VERSION'. Avoid the use of FORMAT or FDISK commands.

If you become virus-infected, it can be very helpful to have backup of your hard disk's boot sector and partition sector (also known as MBR = master boot record). Some anti-virus and disk utilities (Norton Utilities) can do this.

You should also copy these DOS commands from C : \ D O S to the boot floppy disk (as a minimum):

| Filename | Size | Description |
|--------------|--------|----------------------------------|
| ATTRIB.EXE | 11 KB | DOS file attribute utility |
| SCANDISK.EXE | 124 KB | DOS disk space utility |
| FDISK.EXE | 29 KB | DOS hard disk partition utility |
| MEM.EXE | 32 KB | DOS memory display utility |
| MORE.COM | 2 KB | DOS display page pipe utility |
| FORMAT.COM | 23 KB | DOS disk format utility |
| SYS.COM | 9 KB | DOS boot record transfer utility |

TABLE 1. -1 BOOT FLOPPY FILES LIST

You should also copy these additional files to the boot floppy disk for RIT System operation:

| Filename | Size | Description |
|--------------|--------|---|
| APSI2DOS.SYS | 28 KB | SCSI driver |
| APSI4DOS.SYS | 14 KB | SCSI driver |
| APSI7DOS.SYS | 36 KB | SCSI driver |
| APSI8DOS.SYS | 30 KB | SCSI driver |
| APSIEDOS.SYS | 10 KB | SCSI driver |
| APSIDISK.SYS | 13 KB | SCSI Removable Media drive driver |
| APSICD.SYS | 29 KB | SCSI CD-ROM drive driver |
| PKUNZIP.EXE | 29 KB | Unzip utility |
| XCOPY.EXE | 17 KB | DOS file and directory copy utility |
| MSCDEX.EXE | 25 KB | DOS CD-ROM Extension utility |
| HIMEM.SYS | 29 KB | DOS extended memory manager |
| EDIT.COM | 413 B | DOS full screen ASCII editor |
| COMP.COM | 35 KB | DOS file compare utility |
| QBASIC.EXE | 194 KB | Q-Basic Interpreter (req'd by EDIT.COM) |

TABLE 1. -2 BOOT FLOPPY ADDITIONAL FILES

There is a school of thought that your boot disk should also include your anti-virus software. The problem with this is that anti-virus software should be updated frequently, and you may forget to update (and re-write-protect) your boot disk each time. Ideally you will have been sent a clean, write-protected copy of the latest version of your anti-virus software by your vendor/supplier.

When you have everything you need on your boot floppy and any supplementary floppies, make sure they're all write-protected!

What Other Tools Might I Need?

Other suggestions have included:

- Norton Utilities components such as Disk Doctor (NDD). These are not suitable for use by the technically-challenged - any tool which can manipulate disks at a low-level is potentially dangerous. If you do use tools like this, make sure they are good quality and up-to-date. If you attack a 1.0 GB disk with a utility package that thinks 32MB is the maximum for a partition and MFM disk controllers are leading edge, you're in for trouble.
- PKZIP/PKUNZIP or similar compression/decompression utility may be useful both for retrieving data and for cleaning (some) stealth viruses.
- MSD (Microsoft Diagnostic) diagnostic tool supplied with recent versions of DOS and Windows is a useful addition. There are some useful shareware/freeware diagnostic packages, too.

Obviously, these are not all going to go on one boot disk. When you prepare a tool kit like this, make sure all the disks are write-protected!

Tech support types are likely to find that an assortment of bootable disks including various versions of DOS comes in useful on occasion.

If you have one or two non-Microsoft DOS versions (DR-DOS/Novell DOS or PC-DOS), they can be a useful addition. DoubleSpaced or similar drives will need DOS 6.x; Stacked drives will need appropriate drivers loaded.

Note: Support engineers will need to ensure that they are legally entitled to all DOS versions for which they have bootable disks.

How Do I Know I Have A Clean Boot Disk?

You can't usually make up a clean boot disk on a system which has been booted from an infected floppy or hard disk. So how do you know you're booting clean? Actually, you can never be 100% sure. If you buy a PC with the system already installed, you can't be sure the supplier didn't format it with an infected disk. If you get a set of system disks, can you assume that Microsoft or the disk duplicator did not somehow release a contaminated disk image? (Yes, something rather like this has indeed happened...) However, you can be better than 99% sure.

Warning ! You can not make up a clean boot disk on a system which has been booted from an infected floppy or hard disk.

- If you have (and use) a reputable, up-to-date virus scanner, it will almost invariably detect a known virus in memory (scanners can't be relied on to detect an unknown virus, in memory or not). If a good scanner doesn't ring an alarm bell, you've almost certainly booted clean. What constitutes a good scanner is another question.

- If you have a set of original system disks which you received shrink-wrapped and which you've never used or which have only been used write-protected, you can probably use Disk 1 as a boot disk and it probably is not infected - after all, Microsoft doesn't use MSAV for jobs like this. It has been reported, though, that DOS systems disks have been distributed infected, and the fact that they're often distributed write-enabled doesn't inspire confidence.
- You could always contact the supplier of your most-trusted anti-virus utility (or AOS) and ask whether you can send them a boot floppy to check. Of course, even anti-virus gurus sometimes make mistakes, but a boot disk verified in this way would still be worth paying for, especially for organizations with mission-critical systems.

What Are Rescue Disks?

Many anti-virus and disk repair utilities can make up a (usually bootable) rescue disk for a specific system. This needs a certain amount of care and maintenance, especially if you make up more than one of these for a single PC with more than one utility. Make sure you update all your rescue disks when you make a significant change, and that you understand what a rescue disk does and how it does it before you try to use it. Don't try to use a rescue disk made up on one PC on another PC, unless you're very sure of what you're doing or you will lose data.

Note: The RIT System CD-ROM disk contains all of the licensed software, in install diskette image files, for each version of RIT. (See the chapter "Creating Install Disks".) Users should ensure that they have backups of important data files.

Maintaining A Rescue Disk

An up-to-date rescue disk is an important part of taking precautions against viruses. The rescue disk contains important information about your hard disk. Having one could save the data on your disk.

Why Create A Rescue Disk?

If a virus damages boot records (files containing information necessary to start up your computer), you will be prompted to reboot your computer with the disk you made labeled "Norton Rescue Boot Disk. These disks contain a backup copy of all information necessary to restore your computer to an uninfected state. If you do not have a NAV Rescue Disk Set, you may not be able to restart your computer without risk of spreading a serious virus infection and causing damage to other files on your disk.

Here are two good reasons to create and maintain an up-to-date rescue disk:

- If a virus damages the CMOS settings or the startup areas (master boot record or boot record) on your hard disk, you can use the rescue disk to restore this information and gain access to your computer again.

If you do not have a rescue disk, you may have to reformat your hard disk to restore this information, which could mean losing all of the information on your disk.

- If a virus is found in memory, you can use your rescue disk to reboot your computer. Then you can run an anti-virus utility from the rescue disk to find and eliminate the virus.

When To Update The Rescue Disk

You should update your rescue disk whenever you:

- change your computer's partition tables (usually done with FDISK) or logical drive assignments
- modify your AUTOEXEC.BAT or CONFIG.SYS files
- change any of your CMOS settings
- update the virus definition files

How to Create a Rescue Disk

The rescue disks you create using Norton AntiVirus will reside on two disks. In emergency situations, you can use Rescue Disk #1 to boot your computer and restore damaged system files. You can use Rescue Disk #2 to scan for and remove viruses.

Creating Rescue Disks

You will need two newly formatted 1.44MB floppy disks before starting this procedure.

Tip: Since Windows maintains open files and may write to your rescue disk, the RESCUE program may not work properly. Therefore, you should exit to DOS before creating or updating your rescue disk.

Steps To Create Or Update NAV Rescue Disk #1

- STEP 1.** To display the NAV Rescue dialog box type at the DOS prompt:
C:\NAV\RESCUE.EXE
- STEP 2.** To display the Create Rescue Disk dialog box: select **C R E A T E .**
- STEP 3.** Select a drive (usually A:) for the rescue disk in the Rescue Drive drop-down list box.
- STEP 4.** Make sure the appropriate size floppy disk is specified in the Diskette Type drop-down list box.

STEP 5. Check (use the spacebar to check or uncheck options) the following options in the Rescue Disk Contents group box. All other options in the Rescue Disk Contents group box should be unchecked.

- Rescue Utility
- AUTOEXEC.BAT [AUTOEXEC.SAV]
- CONFIG.SYS [CONFIG.SAV]
- Special Recovery Information
- FDISK (Partitioning Program)
- FORMAT.COM

STEP 6. Select Create and follow the instructions on screen.

STEP 7. When the process is complete, remove the floppy disk from the drive, write-protect it, and then label it “Rescue Disk #1”.

Steps To Create Or Update NAV Rescue Disk #2

STEP 1. From the Create Rescue Disk dialog box, uncheck Format Rescue Diskette.

STEP 2. Uncheck Update Changed Files Only

STEP 3. Check the following options in the Rescue Disk Contents group box. All other options in the Rescue Disk Contents group box should be unchecked.

- Norton AntiVirus
- Norton AntiVirus Overlay
- NAV Configuration
- NAV Main Database
- NAV Database Part 1
- NAV Database Part 2
- NAV Database Part 3
- NAV TSR Database Part 1
- NAV TSR Database Part 2
- NAV External Detection

STEP 4. Select Create and follow the instructions on the screen

STEP 5. When the process is complete, remove the floppy disk from the drive, write-protect it, and then label it “Rescue Disk #2”.

Updating Virus Definitions

To prevent newly discovered viruses from invading your computer, you should update your virus definitions files monthly.

Update Virus Definitions Automatically

Norton AntiVirus has made this an easy and simple process. If your computer is connected to a modem or the Internet, click the LiveUpdate button from the Norton AntiVirus main window and the rest is done for you. Just follow the prompts on the screen.

To update virus definitions automatically:

- STEP 1.** In the Norton AntiVirus main window, click LiveUpdate.
- STEP 2.** In the How Do You Want To Connect drop-down list box, select one of the following:
- STEP 3.** Find Device Automatically: Norton AntiVirus determines if you have an Internet connection or must connect using your modem.
- STEP 4.** Internet: Norton AntiVirus connects to the Symantec FTP (File Transfer Protocol) site on the Internet.
- STEP 5.** Modem: Norton AntiVirus dials a preset number and connects to a Symantec server through your modem.
- STEP 6.** Click Next to start the automatic update.

When the update is finished, read the new Text Documents (*.TXT) in your Norton AntiVirus folder that are downloaded also. They contain information about newly discovered viruses and any special precautions that you should take. C:\PROGRAM FILES\NORTON AntiVirus is the usual location for the Norton AntiVirus files.

Update The Virus Definitions Files Yourself

Free monthly virus definition updates for NAV v3.0 are available from:

- Symantec's Internet World Wide Web site: <http://www.symantec.com/>.
- AOS Intranet Web site: <http://www.aos.tc.faa.gov/AOS270/>.

When the update is finished, read the new Text Documents (*.TXT) in your Norton AntiVirus folder that are downloaded also. They contain information about newly discovered viruses and any special precautions that you should take. C:\PROGRAM FILES\NORTON AntiVirus is the usual location for the Norton AntiVirus files.