HOW TO PROTECT YOUR MACINTOSH FROM VIRUSES, TROJAN HORSES AND WORMS ("HEXUALLY-TRANSMITTED DISEASES") USING VIRUSDETECTIVE® AND VIRUSBLOCKADE™ II

by
Jeffrey S. Shulman
(Author of VirusDetective® and VirusBlockade™ II)
and L. J. Shulman

This article appeared in
ICON: the Journal of the Association of Apple 32 Users
January 1991 (Vol. 8, No. 1)

Viruses have been blamed for just about every Macintosh crash since viruses were first discovered. The truth is that the vast majority of Macintosh crashes and problems are NOT caused by viruses, but rather by factors such as corrupt and buggy software, INIT incompatibilities, corrupt files, or bad disks. The purpose of this article is to reduce fear of computer viruses and shed light on what a virus is, what a virus does, how a virus is transmitted, how you can tell if you have a virus, and what you can do to prevent your Macintosh from becoming infected.

HEXUALLY-TRANSMITTED DISEASES

Hexually-**T**ransmitted **D**iseases (HTDs) come in three basic varieties: the virus, the Trojan Horse, and the worm. People tend to group these three together under the one heading of "virus" – this is inaccurate and leads to confusion and misinformation. After you read this article, I hope you will see that a "virus" is different from a "Trojan Horse" which is different from a "worm." Trojan Horses and worms are DEFINITELY NOT viruses, and should not be labelled as such. We shall start with the Trojan Horse.

I will not describe each HTD in detail nor will I describe their symptoms. Information regarding HTDs that is vital for you to know is widely available from other sources. In my opinion, two of the best sources are John Norstad's Disinfectant application and Henry Schmidt's *VIRUS ENCYCLOPEDIA* HyperCard stack.

TROJAN HORSES

The term "Trojan Horse" was taken from the Greek myth of the Trojan Horse. Briefly, for those who are not be familiar with the myth, it is where, long ago, a handful of Greek soldiers hid in the innards of a large, hollow wooden horse. The wooden horse was brought to the gates of Troy. The citizens of Troy became curious and brought the horse within the city gates, at which point the Greek soldiers burst from their hiding place, and opened the gates from inside the walls of Troy. The bulk of the Greek army flooded through Troy's open gates whereby the Greeks conquered the Trojans.

In regard to computer software, a ‘Trojan Horse’ is a stand-alone application that, on the surface, appears to be benign but in fact, when executed, causes damage to your computer disks and files. A Trojan Horse CAN NOT REPLICATE ITSELF and must actually be EXECUTED for damage to disks and files to occur.

The first Macintosh Trojan Horse was found in 1987 in the form of a HyperCard stack which gave every outward indication that its function was to show images of the 'then' new Apple scanner. What this stack REALLY did (besides show poorly-digitized pictures of the Apple scanner) was to plant a virus into the System file (the "MacMag" virus) which, on the 2nd of March, 1988, displayed a message which said "Peace." The Peace Trojan Horse was rather benign compared with the more destructive Trojan Horses that exist: *Steroid, Virus Info, Mosaic, AAVirus and FontFinder.* These five Trojan Horses erase files and wipe out disks – as you can see, they are VERY destructive.

> NOTE: there does exist a legitimate, non-Trojan Horse version of FontFinder as well.

Once discovered, a Trojan Horse can quickly be stopped since it must intentionally be copied from disk to disk for it to spread. If you harbor any files with the above names, you should check it with a competent HTD scanner (read further in this article) and trash the offending file if it is indeed a Trojan Horse. *DO NOT EXECUTE ANY PROGRAM YOU SUSPECT OF BEING A TROJAN HORSE**!***

WORMS

A 'worm', like a Trojan Horse, is a separate, stand-alone application. The difference between a Trojan Horse and a worm is that a worm is designed to replicate itself and spread. Perhaps the most famous worm was the Internet worm which spread to several thousand computers on the Internet nationwide computer network one fine day in the autumn of 1988. A worm may or may not do intentional damage as it spreads. In the case of the Internet worm, the act of replicating was damaging enough. As of this writing, no worms are known to exist for the Macintosh.

VIRUSES

Finally, we come to our nemesis, the 'virus'. A computer virus, like a biological virus, CANNOT LIVE BY ITSELF; it is NOT a stand-alone application. It must find a host to which to attach itself ('insert its code into'). A computer virus is designed to spread and infect other hosts (similar to a biological virus and the above-mentioned computer worm). Besides spreading, the virus is able to do "intentional" damage.

The major differences between a Trojan Horse, worm and virus rest on whether or not each is a stand-alone application, and whether each is able to replicate automatically.

On the Macintosh, none of the existing viruses (nVIR, WDEF, INIT29, CDEF, MacMag, ANTI, Scores, ZUC and MDEF) does "intentional" damage – that is, the virus programmer-creator did not intend for the virus to do the damage it does. Mainly, the real damage is due to things besides intent: 1) the fact that

the virus programmer-creator wrote buggy code, or 2) in the very act of spreading, damage is a side-effect.

> NOTE: the Scores virus did try to attack two specific programs that were never released to the general public.

ACTIVE AND INACTIVE VIRUSES

An ACTIVE virus is the form of a virus that DOES in fact spread and infect files if you were to run the application that contains the virus code.

An INACTIVE virus is the form of a virus that does NOT spread and infect files if you were to run the virus code. An inactive virus results from either a blocked infection attempt (an attempt that began and was aborted before it could complete its work) or a partial REPAIR attempt by some anti-virus program. An inactive virus actually IS the "pieces" or "fingerprints" (technically known as resources) of the virus which were left behind.

nVIR, VIRUSDETECTIVE, ACTIVE AND INACTIVE VIRUSES

The nVIR virus seems to be the one virus that has many variations, the only difference between the variations being the resource type used. As of this writing, there are half a dozen (or so) variations of nVIR.

As you may have noticed from the title of this article, VirusDetective and VirusBlockade II are two programs I wrote; both are distributed by Shulman Software Co. We distribute VirusDetective purposely to find only nVIR's ACTIVE form (that is, the infectious form) as opposed to its INACTIVE (non-infectious) form, the reason being *time.* We distribute VirusDetective with a single nVIR search string that finds all of nVIR's past, present and future ACTIVE resource type variations.

That doesn't mean that VirusDetective is inherently unable to find inactive viruses – IT CAN. It can ***IF*** the user devises a search string to detect each new INACTIVE virus and inserts the search string into his/her own version of VirusDetective. By devising his/her own search strings, the user customizes the search string set according to his/her own needs for HTD protection. No new update of the program is needed, which translates to less expense to you. *YOU the user are in control, not the anti-HTD program's writer, distributor, or manufacturer.*

As I said, the reason our firm distributes VirusDetective to find only nVIR's active form (infectious) as opposed to its inactive (non-infectious) form is *time.* If VirusDetective has a search string for each of nVIR's INACTIVE variations, VirusDetective's scanning time would go UP. This would slow things down a lot. It is my belief that the majority of Macintosh users want whatever HTD protection software they use to be speedy and to catch ACTIVE viruses. The alternative would be to have their HTD protection software be slow and catch both ACTIVE AND INACTIVE viruses. I have left it up to each individual user to

decide for himself/herself between the trade-off that exists between the time VirusDetective takes to do its scanning vs.VirusDetective's thoroughness.

> NOTE: several commercial programs exist where in order for them to detect each new inactive variant of nVIR, the user must obtain a new update of their program, thus more expense and hassle to the user**!**

HOW DOES A VIRUS SPREAD?

A virus can NOT spread by just existing – the machine code that actually contains the virus must be executed. Once the machine code which contains the virus code (hereon simply called the "virus code") is executed, the virus sets up various spreading mechanisms which, for security reasons, I shall not divulge here.

The first and most obvious way for a virus to spread is for you to execute ("run") an application (such as Aldus PageMaker) which has been infected with a virus. What happens is that the virus code is executed first and only after the virus has done its dastardly deeds does the virus execute the real application code. Most Macintosh viruses spread this way.

A question a lot of Macintosh users ask is "if you never actually execute an infected application, is it correct that you can never get a virus**?**" Alas, no, this is not the case. Two more ways exist for a virus to spread.

The second way for a virus to spread is the virus sticks itself into the System file. The System file contains many of the resources necessary in order for the Macintosh to work. Some of these resources are actually real pieces of machine code (called "executable" machine code or just "executables" for short).

A special executable resource type called an "INIT" is run every time you restart ("boot") your Macintosh. Most Macintosh users are already familiar with INITs. INITs are those entities that put icons at the bottom of your screen when you boot your Macintosh. Most INITs are located in the System Folder but outside the System file. A virus (such as Scores and INIT29) places its own INIT resource directly into the System file which is then run along with all the other INITs.

The third way for a virus to spread is somewhat more complicated: the virus masquerades as an executable resource other than an INIT. Technically speaking, some executable resources other than INITs are called DEFinition procedures. These DEFinition procedures are responsible for various functions such as how menus work (the MDEF resource), how windows work (the WDEF resource), and how controls work (the CDEF resource) (two examples of controls are buttons and scroll bars). The Macintosh operating system needs to find these DEFinition procedures whenever it deals with menus, windows, or controls. These DEFinition procedures are normally stored in the System file

and the Macintosh's Read-Only-Memory (ROM).

In order to use the DEFinition procedures, the Macintosh operating system must first locate them. The operating system starts looking for the DEFinition procedures at the beginning of a linked list called the "resource chain." The beginning of the resource chain is usually the application currently being executed; the System and Read-Only-Memory are at the end. The operating system follows each link down the list until it finds the DEFinition procedure it needs.

Furthermore, on each and every hard and floppy disk, there exists a special invisible file called the Desktop file which contains information vital to the Macintosh Finder. When you are in the Finder, the Desktop file becomes the head of the resource chain and therefore is the first file the operating system searches in order to find DEFinition procedures.

Consequently, if a DEFinition procedure gets into this Desktop file somehow (such as by a virus) and the Finder needs a DEFinition procedure to do something like draw a window, the virus DEFinition procedure in the Desktop file will be the one executed BEFORE the one in the System/ROM**!**

Here is a scenario: you have a floppy disk that is infected with the WDEF virus. This virus resides in the Desktop file. You stick the floppy into your Macintosh disk drive when the Finder is active (which is always true under MultiFinder). The Finder immediately opens the Desktop file in order to draw the icons of the files on the diskette. Let's say you also have a window or a folder open on this floppy. The Finder will then proceed to draw this window or folder whereupon it has to use the window DEFinition procedure called WDEF. Which WDEF resource is the Finder going to use**?** Answer: the infected WDEF resource in the floppies Desktop file**!** Thus, the act of inserting an infected floppy into your Macintosh can cause virus code to be executed which thereby spreads the virus onto the other disks you are currently using**!**

> NOTE: with System 7.0 (and later), the Finder will no longer use a Desktop file on hard disks. However, it will still use a Desktop file on floppies. Therefore, while you won't be able to spread a virus (like the WDEF virus) to your hard disk, you could very well wind up executing the virus from an infected floppy.

HOW CAN YOU PROTECT YOUR MACINTOSH FROM HEXUALLY-TRANSMITTED DISEASES?

Besides never turning your Macintosh on and never running any software on your Macintosh, there are a few things you can do to protect your Macintosh from beastly viruses and Trojan Horses. Your best protection is to devise a sound anti-HTD strategy that you put into action regularly. In order for an anti-HTD strategy to be effective, your strategy must apply to: 1) ALL software,

commercial and public domain, your Macintosh comes in contact with; 2) software obtained by any and all ways and means (such as from a floppy or from downloading from an electronic bulletin board).

You may say to yourself, "…but I only use commercial software and never use public domain software or shareware…". I hate to be the bearer of bad news, but it is NOT only public domain software you have to beware of. In the past, several shrink-wrapped, commercial programs have been found to actively spread viruses. As a precaution to protect the user, the major commercial electronic bulletin board services (such as America OnLine, GEnie and Compuserve) screen ALL their software for HTDs BEFORE the user is allowed to get hold of it.

Your first line of defense (if at all possible) is to quarantine ANY new piece of software and run it only from a locked diskette or locked hard drive [an INIT/cdev called VirusBlockade II (details of which are at the end of this article) allows you to write-lock a hard disk or floppy.] You should also check the new software using the most recent anti-HTD protection available.

> NOTE: some software will not run from a locked disk. If not, contact the software manufacturer and request to have added to the next update the capability to run from a locked disk.

Protection from hexually-transmitted diseases comes in three different types: SCANNERS, INTERCEPTORS and REPAIRERS. In order to be protected against HTDs, you really should have at least one SCANNER and one INTERCEPTOR on your Macintosh. A REPAIRER is optional ***IF*** you practice "safe hex" and keep regular backups.

The first type of HTD protection is the SCANNER. A scanner is a utility that "scans" or "detects" files for KNOWN HTDs. A scanning program could easily be called a DETECTOR. The advantage of a scanner is that you don't have to actually execute the virus or Trojan Horse to detect it. The disadvantage is that it can only detect KNOWN HTDs.

With some scanners, you need to obtain an update of the program (usually at additional cost) whenever a new HTD appears. With VirusDetective, you don't need to obtain an update of the program whenever a new HTD appears because VirusDetective lets you, the user, add search strings to customize the program as time goes on. VirusDetective's strong point, its ability to be "programed", "configured", "customized", results in the maximum protection for your Macintosh.

How protected your Macintosh is is only as strong as the DETECTION capabilities of the scanner program you use. Remember, you first have to FIND the offending virus or Trojan Horse before you can replace or repair the

infected file. If the scanning/detecting function is weak, the rest of the program is weak.

Questions to ask when evaluating scanning/detecting capabilities are:

1) How strong or weak is the scanner**?**
2) In order to detect newly discovered HTDs, must I obtain an update of the program or is the program configurable where the user has the power to change the program (such as by way of search strings) without having to obtain a new update of the program**?** If so, how much is each update going to cost me**?**
3) How good is the customer support**?** Can I call or write to someone if I have questions in regard to a particular program and receive a definitive answer in a timely manner**?**
4) How up-to-date is the program**?**

The second type of HTD protection is the INTERCEPTOR. An interceptor is a utility that "intercepts" or "stops" any action "that spreads or does damage." An interceptor is a generic "stopper" and protects against what HTDs do in general (which is to spread and/or do damage), and does not have anything to do with any particular HTD (including currently 'unknown HTDs'). The advantage of an interceptor is that an interceptor attempts to stop the action of any HTD, including a brand-new HTD that a scanner may not have been programed to detect yet. The disadvantage is that you actually must execute the HTD code; quite often damage occurs.

If your interceptor doesn't work correctly (such as there's a bug in the interceptor) or if the virus gets past the interceptor, your Macintosh will become infected. Some virus programmer-creators (whoever they may be) purposely program their virus code to get around the various anti-HTD interceptors.

Regarding REPAIRERS. It is ALWAYS preferable to REPLACE rather than REPAIR an infected file due to the fact that a virus can damage a file in *subtle* ways. I cannot emphasize this enough. *The act of repairing is NOT completely a safe practice*.

As I mentioned earlier, your best protection is to devise a sound anti-HTD strategy. A sound anti-HTD strategy would be to have BOTH a SCANNER and an INTERCEPTOR in use AT ALL TIMES (as I mentioned, a REPAIRER is optional ***IF*** you practice "safe hex" and keep regular backups). The good news is that superlative anti-HTD tools DO exist for the Macintosh for moderate fees (shareware), and sometimes at no cost at all. Or you can use one of the commercial anti-HTD programs for higher prices with little or no increase in ability to catch and repair HTDs.

Many shareware anti-HTD programs are no less reliable than their commercial counterparts. In the anti-HTD Macintosh arena, *it just ain't true* that the available commercial software (combined with its customer support) is better than the available shareware (combined with its customer support). Don't decide to use a commercial anti-HTD program simply because it's commercial.

Besides VirusDetective + VirusBlockade II (which of course I am partial to because I wrote them), I recommend the following:

1) John Norstad's Disinfectant INIT and application, and
2) Chris Johnson's GateKeeper and GateKeeper Aid.

In regard to scanners, I of course recommend VirusDetective. VirusDetective's advantages are that: 1) it is user-configurable (user-customizable); 2) it is a desk accessory (available at all times to scan a file or disk); and 3) it is a fully-supported product to ***REGISTERED*** users (which includes notification of new anti-HTD search strings, major updates and bug fixes; telephone support when you get stuck or have questions; acknowledgement and implementation of suggestions and needs).

VirusDetective was the FIRST Macintosh anti-HTD program to be user-configurable which negates the need for the user to obtain a new version of the program for each new HTD (or each new variation of an HTD). As each new HTD is discovered, Shulman Software Co. notifies ALL of its ***REGISTERED*** users of what the new search string is in order to combat that HTD. The user then inserts that new search string as data into his/her existing version of VirusDetective.

As a desk accessory, VirusDetective must be OPEN for it to do its detecting. However, when VirusDetective is used with its companion product VirusBlockade II, an INIT/cdev, VirusDetective can automatically be set up to scan floppy disks as you insert them into your Macintosh (there are lots of other bells and whistles).

At this writing, VirusBlockade II Version 2.0 is in its alpha-test stage. By the time you read this article, VirusBlockade II 2.0, with its many enhancements, may already be available.

In regard to recommending an interceptor, it's a little trickier. The very first interceptor was Vaccine from the noted software author, Don Brown. The main problem with Vaccine is that it has not kept up with the times; it has not kept up-to-date. Anonymous virus programmer-creators have recently written viruses to bypass Vaccine's protection. Therefore, Vaccine is not recommended.

A much better quality interceptor is the GateKeeper INIT (not to be confused with the GateKeeper 'Aid' INIT). GateKeeper was written by Chris Johnson and is free of charge. I highly recommend its use. Novice Macintosh users,

however, may find it to be too complicated.

An interceptor that is easier to use than GateKeeper is the Disinfectant INIT that comes with the Disinfectant application. Disinfectant is not an interceptor as I have defined it above. It is not a generic “stopper” that protects against what HTDs do in general; it only intercepts “known” viruses. It’s an interceptor only in the sense that it will stop specific virus, not viruses in general.

If you regularly scan all new files, then the Disinfectant INIT is doing nothing that you aren’t already doing and won’t detect any new viruses.

At this time, you should also add to your anti-HTD arsenal Chris Johnson’s GateKeeper ‘Aid’ INIT (different from the GateKeeper INIT mentioned above) which is also free of charge. The GateKeeper Aid INIT protects your Macintosh from viruses that invade the Desktop (such as the WDEF virus) and automatically removes any Desktop viruses it encounters.

The capabilities of VirusBlockade II 2.0 include protecting your Macintosh from viruses that invade the Desktop and will automatically remove any Desktop viruses it encounters. You don’t need both GateKeeper Aid AND VirusBlockade II 2.0.

HORRORS! MY MACINTOSH HAS IN FACT BECOME INFECTED WITH A VIRUS OR TROJAN HORSE!

You thought you took the proper precautions but somehow your Macintosh has in fact become infected with an HTD. What do you do **?** The number one thing is “DON’T PANIC**!**”

If you have a virus that infects the Desktop file (like the WDEF virus) of your hard disk, it is a relatively easy procedure to eliminate the virus (or “clean” the disk): you instruct the Finder to rebuild the Desktop file. Just prior to rebuilding the Desktop, It is a good idea to turn off MultiFinder.

All you do to rebuild the Desktop file is hold down the Command and Option keys while you restart your Macintosh. Keep these two keys down until a dialog box appears asking you, “Are you sure you want the desktop rebuilt on disk ‘X’ ? (This may take a few minutes.)” Click OK.

Not only do you have to eliminate the virus on your hard disk, you must eliminate the virus on any and all floppies that may have become infected; rebuild the desktop on any and all suspected floppies. If you do not “clean” your floppy disks, the act of inserting an infected floppy disk into your Macintosh will spread a Desktop virus to your hard disk all over again.

When you are finished “cleaning” all hard disks and floppy disks, turn MultiFinder back on.

HIGH PRIORITY: REPLACE INFECTED FILES FROM YOUR BACKUPS

IT IS VERY IMPORTANT TO BACK UP YOUR FILES**!** *I cannot stress this point enough**!*** If your Macintosh has a virus that infects various applications or the System file, the best thing you can do is retrieve the non-infected application or System file from your clean BACKUP or from your ORIGINAL MASTER diskettes. Be sure to physically write-protect your backup and master diskettes *BEFORE* you insert them into your Macintosh**!**

> NOTE: to physically write-protect a diskette, turn a diskette around so you are looking at the back of the diskette. The tab should be in the 'up' position which leaves a hole (of sorts) in the diskette. If you can see through the hole, it is write-protected. If you cannot see through the hole, an HTD can get to the diskette.

IF YOU MUST REPAIR…

If you don't have any un-infected backup (or have old backup or no backup at all) or master diskettes, the next best thing is to use a virus REPAIR program.

I must repeat that it is ALWAYS preferable to REPLACE rather than REPAIR an infected file due to the fact that a virus can damage a file *in subtle ways. The act of repairing is NOT completely a safe practice.*

I recommend the Disinfectant application (not the INIT); in my opinion, it is the best REPAIRER. It is free of charge.

For the future, I *HIGHLY* recommend you make the commitment of resources and time to BACKUP your disks on a regular basis. I don't think you'll regret it…

YOU THINK YOU DISCOVERED A 'BRAND-NEW' VIRUS

Your Macintosh has been acting strangely. Perhaps it keeps crashing or doing other "funny" things. You've used all the latest anti-HTD checkers and they show nothing is wrong. Aha **!** You've must have discovered a new virus **!** Nope, 'tis not so. In 99% of the cases, you have NOT found a new virus.

*If it isn't a new virus, then what can it be**?*** It could be any number of things. Did the symptoms start when you just added a new piece of software or an INIT**?** Did you recently update your System**?** – if the answer is yes, start there. Or…

…have you lately turned off your Macintosh without first doing "Shut Down" from the Finder**?** Has your Macintosh crashed lately**?** The Macintosh keeps valuable information in its memory at all times in regard to the current status of open files on your disk. This up-to-date information gets permanently recorded onto the disk only on certain occasions, such as Shut Down and Restart.

When you turn your Macintosh off without first doing Shut Down, or your Macintosh “spontaneously” crashes, the information that once was in memory is lost forever because it was ONLY in memory and never got a chance to get recorded on disk – chances are good that the open files are now corrupt. One of the open files was the all-important System file. Guess what happens when the all-important System file becomes corrupt**?**

The Disk First Aid utility by Apple lets you diagnose whether a disk has one or more corrupt files on it. Disk First Aid will try to repair your disk but it is not always possible for it to do so. You could also try one of the commercial disk repair utilities. If these fail, you will have erase that particular disk (whether your hard disk or floppy) and restore the files from the BACKUP disks you have. If you do not have backup disks, you may have irretrievably lost everything**!**

If the Finder (you are in the Finder whenever you are not using an application like Claris MacWrite II) is acting strangely (two examples of strange would be you cannot copy a file or directories disappear), it could be that the Desktop file is messed up. Try rebuilding the Desktop by following the above-mentioned instructions. It is a good idea to rebuild the Desktop occasionally anyway in order to clean out garbage the Finder doesn’t remove whenever you delete a file.

> NOTE: when you rebuild the Desktop, you will lose any comments you typed into the “Get Info” box.

If a specific application is troublesome, then try replacing it from its original, locked, master disk.

Random non-specific problems (‘things are not working right’) occur whenever the all-important System file becomes corrupt (or for that matter, any other file in the System Folder). To fix random non-specific problems, re-install a fresh copy of the System and Finder by using your original Installer disks from Apple.

Before you re-install the System and Finder:

> *Step 1: use the Font/DA Mover to save any fonts and desk accessories you want re-installed;*
> *Step 2: you may also want to replace your INITs (and the like) with fresh copies;*
> *Step 3: delete the OLD System (if you don’t delete the OLD System first, problems can still happen);*
> *Step 4: finally, re-install the System and Finder.*

Are you still convinced you have a virus**?** Try looking for characteristic “virus” activities. One characteristic virus activity is when a file substantial increases in size. As a virus infects a file, it has to add virus code to your file thus the

virus usually causes an increase in the size of that file.

Immediately after you have re-installed the System and Finder, and rebuilt your disk's Desktop, use the Finder's "Get Info" command to record the number of bytes of the System, Finder, the applications you use most often, and each file you suspect to be infected. When problems start happening, make note of any substantial changes in size (about thirty bytes or more). The System will change by a few bytes when, for example, you change your Chooser name or selections; this is normal (don't worry about it).

If you see substantial changes in size, you may indeed have yourself a virus. If you are an 'advanced' Macintosh user (this is definitely not for the novice or even intermediate-level user), you might use ResEdit. ResEdit is a tool which will let you see if any new resources have been added to your files.

> NOTE: ResEdit is a VERY, VERY powerful program. Seriously – with ResEdit, if you don't know what you are doing, *don't do anything***!** Don't play with ResEdit**!** With ResEdit, I kid you not, you can screw up your Macintosh far worse than any virus can**!**

Rather than experiment with ResEdit, send your suspected files to me and I will look at them. My U.S.P.S. address and electronic mail addresses are listed at the end of this article.

YOUR BEST WEAPON IS TO STAY INFORMED

In conclusion, the best protection against HTDs is to stay informed with the latest news.

The best ways to stay informed are to …

1) … join the Macintosh Special Interest Group (SIG) connected with one of the three major, international, commercial electronic on-line bulletin board services (BBS): America OnLine, Compuserve or GEnie. These three services screen all software to prevent HTDs from being passed to their users.

2) … join a national Macintosh user group. I would recommend either BCS•Macintosh (Boston Computer Society) or BMUG (Berkeley Macintosh User Group). Both run electronic online bulletin board services for their members. These two groups screen all software to prevent HTDs from being passed to their users.

3) … join the Macintosh Special Interest Group (SIG) connected with your local computer user group.*

4) … join a local electronic bulletin board service.*

* *Investigate ahead of time whether the particular local Mac SIG or*

> *BBS you are thinking of joining screens the software that passes through them on a regular and consistent basis. This service is a definite PLUS; you may even consider it so important as to be a MUST. The screening of software prevents HTDs from being passed on to unsuspecting users.*

In regard to VirusDetective, within days of the discovery of a new HTD, whether it be a virus, Trojan Horse or worm, Shulman Software Co. notifies all ***REGISTERED*** VirusDetective users by mail of the fact that a new HTD has been discovered and what the appropriate search string (or search string combination) is to combat the new HTD. This customer support is one that we perform as a usual part of our follow-up.

Within hours of the discovery of a new HTD, in addition, we post those same search strings on four major electronic bulletin board services (Compuserve, America OnLine, GEnie and Delphi).

In writing this article, my goal will have been reached if the article sheds light on what hexually-transmitted diseases are, what they do, how they are transmitted, how you can tell if your Macintosh has one, and what you can do to prevent your Macintosh from becoming infected by one. I hope it has become clear how VirusDetective and VirusBlockade II relate to HTDs.

It’s unfortunate, sad and perhaps pathetic that promising Macintosh programmers feel they must make their mark on the Macintosh community by writing destructive HTDs instead of constructive software. It would be nice if viruses, Trojan Horses and worms had never been written; therefore, I never would have had to write VirusDetective and VirusBlockade II. Unfortunately, “us” users were never given the choice.

VIRUSDETECTIVE AND VIRUSBLOCKADE II

VirusDetective®…

is a desk accessory that unearths and sniffs out viruses and Trojan Horses BEFORE they get a chance to lay waste your Macintosh by looking for the “fingerprints” viruses leave behind. PREVENTION IS THE BEST CURE! Customizable (change, add or delete) search strings. Read search string list from a word processing file, or write list to text file; also appends. Choose your own word processor 'text' file formats (such as MacWrite II). Create your own search strings. Can write logs of all files, or only infected files. Status box includes progress bar. When in midst of scan, telltale sign is its "four-diamond" cursor. Automatically scans whole bunch of floppy disks (one after another) or on individual, “as needed” basis. Gives detailed technical info of infected files.

Protect settings from tampering via password. Full internal Help files; copy to Clipboard. Unattended operation. System 7.0 Balloon ‘Help’. When a virus is discovered, we provide the search string which get posted to major electronic bulletin boards and mailed to all registered users. Elegant new “look & feel”. A pleasure to use. And much more!

Minimum requirements: Mac Plus; System 6.0.2. System 7.0 friendly.

PRICE of VirusDetective: $40 US/$45 non-US.

30-day money back guarantee. Site licensing available.

VirusBlockade II™ (comes bundled with VirusDetective)…

Together, VirusBlockade™ and VirusDetective form a revolution in Macintosh anti-virus protection! VirusBlockade gives you the means to direct how, when, and where VirusDetective does its searches.

Steve Bobker, Contributing Editor, MacUser magazine, said this about them: “VirusDetective 5.0 and VirusBlockade II [2.0] have soared to the top of the antivirus heap. Awesome.”

SUPERFAST FILE SCANNING searches a file as soon as the file gets inscribed onto the disk (which means whenever you DOWNLOAD, SAVE, COPY, or UNCOMPRESS a file; more technically, whenever "any file is created" or "any resource is changed"). SUPERFAST FILE SCANNING is definitely a MUST-HAVE for anyone who downloads or copies files from networks. SUPERFAST FILE SCANNING even works on FILE SERVERS!

Henry Norr wrote in an article in MacWeek (Oct. 8, 1991, Vol. 5, No. 34, p. 6): ‘The result is “a network manager’s dream come true,” said Geoff Hartley, a Hollister, Calif.-based software and networking consultant and sysop in charge of Mac virus information on the Computer Virus Industry Association’s electronic bulletin board.’

Then there is the ROOKIE SWITCH! Have you ever worried about (with good reason) a UNknowledgeable user letting a virus onto a Macintosh, usually by NOT knowing what to do when a message comes up on the screen warning that an infected file has just been found? With the ROOKIE SWITCH, anytime VirusBlockade finds a virus or Trojan Horse that is about to infect the Macintosh, the screen freezes and a message appears telling the rookie-user (s)he cannot proceed and to consult the designated "experienced" Mac person who then gets rid of the imminent infection competently. RESULT: no infection, and the rookie-user continues his/her work.

What else is new? VirusDetective and VirusBlockade have a totally redesigned "look and feel". Scan floppy disks "if you don’t hold down a particular key" (the most requested feature). Selectively scan any disk when disk is started up or

mounted, or scan on a specific day of the week, or on a specific day of the week and time of day. When a "desktop virus" (like WDEF) is encountered, it is automatically removed. When an infection is found, you can be alerted, have the infected file deleted, renamed, or moved to a top-level folder of your choice. Of course, it still lets you automatically write-protect disks; scan floppy disks as you insert them; have floppy disks ALWAYS eject as soon as they are inserted. And much more...

Minimum requirements: Mac Plus; System 6.0.2. System 7.0. friendly. VirusBlockade requires VirusDetective.

PRICE of VirusBlockade (VirusDetective is included in this price): When you order both programs together, $59 US / $64 non-US.

VirusBlockade comes bundled with VirusDetective. Youmay purchase VirusBlockade ‘concurrently’ with or ‘after’ VirusDetective, but not ‘before’ VirusDetective.

30-day money back guarantee. Site licensing available.

COMPANY INFORMATION

software written by Jeffrey S. Shulman

owned and distributed by
Shulman Software Co.
1111 W. El Camino Real, Suite 109MAC, Sunnyvale, CA 94087-1057 USA

Phone:	408/245-1890
FAX:	408/245-1891
Office hours:	Mon - Fri 9am - 5pm (Pacific Time)
Technical Support hours:	Mon - Fri 9am - 8pm

Electronic addresses:

America OnLine:	KILROY7
Compuserve:	76136,667
Delphi:	JEFFS
GEnie:	KILROY
AppleLink:	KILROY

VirusDetective and VirusBlockade are distributed worldwide via direct-mail through Shulman Software Co., a commercial enterprise.

HOW TO ORDER

Orders must be accompanied by payment-in-full at the time of order in the form of a check, international money order, Visa or MasterCard. Make check/money order out to SHULMAN SOFTWARE CO. Monies must be in US currency with check drawn on a US bank, or international money order. No billing, no COD's – this functions to keep costs down which we pass on to our customers.

30-day money back guarantee… if you are not completely satisfied, we will gladly refund your money.

Prices subject to change without notice – call or write to verify current prices.

- the end -