



MAC FACTS

from

Mac Help Desk

SUPPORT, SALES, TRAINING & SERVICE

(972) 783-9787 • (972) 783-7550 - *Fax/Modem* • (214) 249-9543 - *Pager*

e-mail address - machelpdesk@home.com

Web site - www.machelpdesk.com

Volume 8, Number 7

July 1999

A Message from Dru

Hope your 4th was as much fun as mine was. Spent Saturday July 3rd with Mom (visiting from FL.) and family at Addison's Kaboom Town. Sunday the 4th saw us at another great display at Breckenridge Park in Richardson. Is it me, or did the fireworks look particularly good this year?

○*****▼▲ *△○**●

I mention, in passing, that Charles Caffey has left the employ of Mac Help Desk. After almost four years of service, I felt it was time for Charles to exercise other opportunities. I wish him the best of luck in all his upcoming endeavors.

○*****▼▲ *△○**●

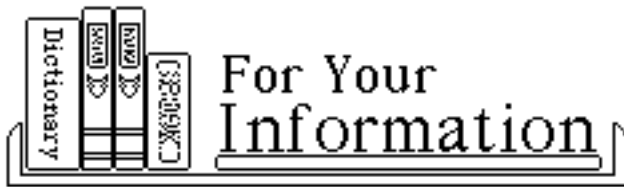
June was **HOT**! But not hot enough to keep us from these new friends – Lenore (Lenny) Parens, Leanne White, Joanne Bond, Blue Green Southwest, Aaron Smith, Brian Mayes, Piranha Design, Don & Peggy Crabtree, Dal Truck, Tommye Cowan, Marina Johnson, Debbie Frankfort. Howdy y'all!

○*****▼▲ *△○**●

It pays to listen in – As I have been mentioning over the past few months, I have a radio show on WBAP (820 on your AM dial). It's called CyberLine [<http://www.cyber-line.com>] and airs every Sunday evening from 7 – 9 pm. The last Sunday of each month is Mac Mania night - a two-hour, no-holds-barred Mac free-for-all. The next Mac Mania is July 25th and we'll be talking about MacWorld. Why am I telling you all this? Because last month we gave away a \$100 gift certificate from Newer Technology to Mac Help Desk client/friend Steve Kaufman and an Epson 740i to Mac Help Desk client/friend Cherly Rios. Listen each month and we'll be giving away more great prizes! Boy, do I love giving stuff to 'my' friends.

○*****▼▲ *△○**●

Have you seen *Star Wars – The Phantom Menace* yet? Like a good laugh? Go to <http://www.sagabegins.com> and view Weird Al Yankovic's epic ode to Star Wars. You'll need QuickTime 4.0 to view and if don't have QT4.0, you can download it at <http://www.apple.com/quicktime>. Well worth the time and effort. Move over Don McClain!



VIRUSES ON THE MAC - A PROBLEM OR NOT?

by Todd Stauffer

VIRUSES

Historically, the Mac has only had to deal with a relatively small percentage of viruses compared to the number that have been created to infect Intel-compatible computers. In fact, there's a certain line of thinking out there that says Mac users are almost so statistically unlikely to encounter a virus that making a big deal out of them is unimportant.

I'm not quite in that camp. For one thing, the fast and furious pace at which the Internet is becoming a part of most Mac owners' computing experience makes for a solid opportunity to distribute viruses. And the Mac isn't exactly impervious; the lack of viruses is probably more the result of a lack of interest than it is in the security of the operating system or some other inherent Mac advantage. There are more viruses on the Intel-compatible PC platform because there are more computers to infect, thereby allowing these virus authors to cause more trouble.

However, more viruses are appearing on the Macintosh -specifically, viruses that are cross-platform. The Microsoft Visual Basic for Applications macro viruses (probably the type you're most likely to encounter in the near future) can hop right from a Windows-based PC onto a Macintosh running Microsoft Office. It's likely that other cross-platform viruses, perhaps written to exploit holes in Java (a technology that allows programs to run on many different operating systems) or other cross-platform solutions will be just as capable of infecting the Mac as any other computers.

So, the threat is real. My Mac has gotten only a few viruses that I'm aware of, and all of them (again, all the viruses I've caught) were either Microsoft macro viruses or viruses specific to a particular application (for instance, HyperCard-based viruses). Other than that, I've been lucky. Still, surfing the Internet, sharing floppies, swapping Zip disks, and sitting on a large computer network are all high-risk activities that leave you more susceptible to viruses.

WHAT IS A VIRUS?

First and foremost, a virus is a program, and its main goal is to replicate itself as much as it possibly can. It wants to copy itself onto new hard drives, new removable media, and new computers over networks. Viruses are often designed to infect low-level operating system code so that they can self-replicate whenever certain commands are invoked on the computer or when a particular event, such as a new floppy disk being inserted or a new computer appearing on the network.

Viruses can be malicious, but they don't have to be. Many viruses are relatively harmless; they self-replicate and try to distribute themselves to more and more computers, but then at some prescribed date and time, they pop up season's greetings or peace messages on screen. Still other viruses are designed to be annoying by moving the cursor around the screen, popping up dialog

boxes, or affecting the display. Of course, these can still cause problems as there's a good chance they'll crash an application or the entire system, potentially affecting data.

The worst viruses are those that attempt to destroy data and files on your Mac. These viruses may try to infect the hard disk driver software, the system software, or even the desktop database. They erase files, mess up your folders, and attack the disk's structure itself, introducing errors. In some cases, they can manage to erase or mangle your entire hard drive. It's very rare that this happens, especially on a Mac, but it can happen. (See Table below for a list of some Mac viruses.)

SAMPLE MACINTOSH VIRUSES

Virus	Virus What It Does
Autostart 9805	Exploits a hole in QuickTime to copy itself to available disk volumes, and then creates invisible files on the hard drive. Causes extensive disk or network activity and can overwrite some files with bad data. (Technically a worm, not a virus -see the sidebar "Non-viruses: Other malicious code.")
Code 252	Infects applications and some system files. Displays a message that says, "You have a virus. Ha Ha Ha. Now erasing all disks...[etc.]" before deleting itself. Does no other damage on purpose, although it can crash the machine and cause damage.
Init 17	Displays the message "From the depths of Cyberspace." It's been known to do some damage, especially to 68000-based Macs.
Init 29 Init 29, cont.	Infects all types of files and spreads rapidly on the system. May display the following message when a disk is inserted in the floppy drive: "The disk needs minor repairs. Do you want to repair it?" Can cause many unintentional problems.
Init 1984	On Friday the 13th, the virus damages files by renaming them, changing file dates and sometimes deleting files. Infects system extensions only. (Init-M is a similar virus.)
nVIR B	Infects applications and the System file, but does no significant damage. Has a number of strains, including AIDS, CLAP, Hpat, Jude, nFlu. Will sometimes beep or say, "Don't panic" if speech is enabled.
MDEF	Infects the System file, doing no intentional damage. Can cause crashes. Has a number of strains, including Garfield, Top Cat, C, D.
T4	May keep extensions from loading or make the hard drive unbootable (depending on the version number). Strains include A, B, and C.
Zuc	Causes the mouse pointer to move around on the screen whenever the mouse is held down and an infected application is running. Only infects applications

NON-VIRUSES: OTHER MALICIOUS CODE

Along with viruses, which are self-replicating programs that attach themselves to other programs, there are two other major types of problem programs -Trojan horses and worms. A Trojan horse is rogue code that (probably) does something malicious, but is disguised as a program that does something interesting. An example would be a program that says it will get you free Internet access but actually erases your hard drive when executed.

Worms are even more like viruses -they're self-replicated, but they don't attach themselves to programs. Like viruses, they're sometimes malevolent and sometimes they don't do much of anything. An example of a worm is the AutoStart 9805 worm.

The AutoStart 9805 worm only affects Power Macintosh systems. Using the AutoStart feature in QuickTime 2.0, 2.5 and 3.0, the worm launches itself when an infected disk or other media is mounted on the Mac's desktop. If that Mac isn't already infected, the worm copies itself to the Extensions folder as a program called Desktop Printer Spooler. Now whenever the Mac is restarted, this worm program is run.

After infecting all the drives it can, the worm looks for files ending with "data", "cod", and "csa". When a targeted file is found, it is damaged by the worm overwriting the data fork with random data. The current workaround is to disable AutoStart in the QuickTime control panel, although the major Mac virus detectors are capable of detecting and destroying the worm.

WHAT'S NOT A VIRUS?

There are a number of hoaxes out there that seem to be forever circulating on the Internet. Some people compare them to "urban legends": stories such as the one about the little boy who wants postcards before he dies from leukemia or the frantic warnings about body parts being farmed by prostitutes. These chain-mail type ventures are very popular in e-mail.

Some of these e-mail hoaxes show up in the form of virus alerts that have been released by the U.S. government, Microsoft, a university, or some other organization that seems credible. Surprisingly, most of the alerts I've read have glaring misspelling and grammatical errors that seem to indicate that they're hoaxes, but that deters few people.

When one of these notices arrives in your In box, don't forward it, and don't believe it. Unless you've heard otherwise from a very reliable source, the following statements will always be true about viruses:

- * Regular, text e-mail messages cannot be infected with a virus.
- * A virus is almost always distributed by attaching itself to a program, which can be an attachment to an e-mail message. The infected program must be executed, however, before the virus can infect anything.
- * Unless it's exploiting a security hole in your Web browser, a virus can't be executed simply by loading a particular Web page.

You really shouldn't worry at all about the possibility that a virus is being transmitted through an e-mail message. Instead, you should focus on being sure that files you download from Internet sites and unsolicited e-mail attachments don't have viruses. (You can also suspect a floppy disk given to

you by a colleague or friend if viral symptoms show up in your Mac.) Get a good virus-protection program and scan files you think may be a problem before you launch them.

Note: You'll hear many pundits say that a text e-mail can never be infected with a virus. And, in the current state of technology, that's completely accurate. The problem I have with this blanket statement, though, is it's always possible that some form of scripting or macro language will be popularly instituted by e-mail programs, at which time a virus infection -such as by the Word macro virus -may be possible. Javascript, for instance, is a scripting language that consists of text commands embedded in Web pages. These commands turn Web pages into running programs. As long as the host applications themselves remain secure (Web browsers won't allow anything but the most innocuous data to be saved and executed on your Mac by a remote site), you won't have any problems. But if an e-mail application comes along that processes text-based scripting instructions and allows access to the user's hard drive (through a bug or by mistake, as with Word Basic), e-mail messages could, ultimately, contain viruses or Trojan horses.

VIRAL SYMPTOMS

Although virus authors tend to do their best to hide their viruses (at least until they want them to be found through a dialog box or file damage), there are some symptoms that you can associate with a virus, assuming you've eliminated other troubleshooting possibilities. Although you should always have a virus checker handy, especially to investigate odd behavior, remember that it's far more likely that your problem is related to an extension or hardware conflict, program bug, or file corruption.

That said, here are some symptoms that might suggest a viral infection:

- * You experience seemingly automated behavior on your Mac that can't otherwise be explained (such as files moving on their own, the mouse pointer being affected, dialog boxes appearing).
- * A launched program doesn't appear or appears after a significant and unusual delay.
- * The system unexpectedly restarts after accepting a disk, running a program, or mounting a removable media disk.
- * Extensive, unexplained disk activity occurs, especially when no programs are running and/or when the Mac has been started with extensions off.
- * Files and folders become corrupted or disappear.
- * File sizes, creation dates, names, or other file details change automatically.

In general, these situations describe the action of viruses at the Mac OS level. Program-level viruses do more specific things, usually messing with your ability to use that program. HyperCard viruses infect HyperCard programs, for instance, whereas Word Basic viruses affect your ability to use Microsoft Word correctly.

DETECTION AND CLEANING

If you're a high-risk, connected Mac user, you should consider getting yourself a virus-protection program. These programs generally run in the background, checking files as they appear on your hard drives or in a removable media device. You can also program them to check for viruses at specific times during the day and/or week. Popular antivirus programs include the following:

* Symantec , makers of Symantec Anti-Virus for Macintosh

* Dr. Solomon's , makers of Virex for Macintosh

When a virus-protection program detects an infected file, it will generally try to isolate that file by letting you know it has a problem and, sometimes, giving you the option of moving the file (perhaps to a folder of infected files to help you keep track of them). You then have the option of simply deleting the files and restoring them from a backup (after testing the backup for viruses) or trying to clean the virus from the infected file.

Cleaning is something you should worry about only if you absolutely must have the file's contents -otherwise, I'd recommend deleting and then restoring the file, because most infected files are applications or system files that can be replaced. If the infected file is a document, you might be desperate to get it clean. Run the virus cleaner and see what happens.

Should you run the virus program all the time to check files? If it annoys you, I recommend you back off to scheduled virus sweeps that occur once or twice a week, as long as they work logically within your backup schedule. (Make sure you rotate your backups so that viruses can be dealt with using backup copies of documents and applications.) If you don't mind the additional protection, keep the virus program running. It can't hurt.

The only thing that can hurt is not updating your virus definitions. The major virus-protection publishers come out with updates every few months (sometimes every month) that include more virus definitions, better weapons, and protection from new viruses. Stop by the virus program publisher's site and update frequently.

WORD BASIC VIRUSES

The Word Basic macro viruses are a strain that infect Word documents by infiltrating the Normal template. Using Word's built-in customization and macro abilities, these viruses subtly change Word's behavior, causing both minor and major problems. What's worse, you're only likely to discover this after the virus has been in Word for a while, possibly even spreading the virus by distributing infected documents.

Note: Actually, these macros are often called Visual Basic for Applications macros because they can affect a few different Microsoft applications, including Microsoft Excel. Although the Word macro viruses are much more pervasive, you may find that an occasional Excel document acts oddly. Check that document with a virus checker.

The regular Concept virus - the first one to really appear on the scene - forces your documents to be saved as templates, which are difficult to work with. The virus remains in the newly saved template file, infecting the next computer to which the file is transmitted.

The solution is to download the Macro Virus Protection Tool from Microsoft's Web site. Run the tool according to the instructions that come with it. This tool basically adds a capability to Word that prohibits macros from automatically running if they're in new documents. Now, whenever a file comes up with a macro attached to it, a dialog box will appear that allows you to save the file again, while Word strips the macro from it.

Note: This capability is built into Word 98. By default, Word 98 will ask you if you want to run macros embedded in a Word document. If you don't know why the document would have macros (or if the document is otherwise foreign to you), choose not to load them.

Unfortunately, that solution doesn't work well for another strain, the CAP virus, because it manages to infiltrate the Normal template itself, intercepting any attempts to alter the templates attached to files -which means the Microsoft virus protection tool can't even be loaded.

To get around this one, you'll need to be a little creative:

1. Close Word.
2. Find the Templates folder and move the Normal template to the desktop.
3. Restart Word.
4. Use the File > Open command to find the document you want to load.
5. When you find the file, hold down the Shift key and click Open.
6. Keep the Shift key down as the file loads (this disables macros).
7. Save the file with a new name.
8. Delete the file.

This works great when it works, but even newer strains seem to affect the Shift key macro disabling, making it impossible to load a cleaned version of the file. The only solution seems to be to drag out the Normal template, and then avoid loading the infected files into Word. The next time you open Word, a clean Normal template will be created, and you can go on about your business. Meanwhile, toss the infected documents.

If you don't toss those documents, don't ever open the infected documents again in Word 6.0. You'll also need to search your drive and find any documents that have turned into Microsoft Word Template files (*.dot) instead of regular Microsoft Word files (*.doc). Check the icon, which is slightly different for a template file.

If you absolutely must get the data out of the documents, you might try copying and pasting the document's contents into a different application, and then cleaning out the Normal template and going from there. Or, open the file through ClarisWorks and let it (or MacLinksPlus) translate from Word's template file format. Even if you can't open the file directly, you can try opening it as an RTF file. This may allow you access to the text inside the file so you can copy and paste it into another document. I stress, though, that you don't load the file at all back into Word. It'll infect the Normal template again, and you'll have to start over.

You may have some luck with the very latest virus checkers -Symantec, Network Associates, or one of the others that specifically treats Word Macro viruses. Unfortunately, they probably can't wipe the virus from a particular file; they can just help you determine that the file is infected. You should also have luck opening most of these infected files if you upgrade to Word 98 or higher.

This sort of virus is particularly insidious, because you'll likely end up tossing the infected documents, and you may have been working with infected documents for quite a while. Luckily, the problem is limited to the documents themselves -no directories, applications, device drivers, or anything else will have been infected. These macro viruses offer a great reason to keep a good backup of your documents.

NEWSLINE

Future Power Steals iMac Design

A small PC vendor from Santa Clara, California is doing what larger corporations dare not to – blatantly stealing patented designs from Apple Computer, Inc.

On Tuesday June 22nd, Future Power announced their "E-Power" personal computer, which can be mistaken for Apple's iMac any day. According to Future Power employees who were working their booth at this week's PC Expo in New York City, the unit will ship with a 466MHz Celeron processor, a 40X Sony CD-ROM, a 3Com 56Kbps V. 90 modem and 64 MB of SDRAM.

Additionally the PC will pack dual USB ports, a 6.4GB Ultra DMA drive, a single PCI slot, a NEC floppy drive, a Diamond Multimedia 8MB 3D AGP card and a built in 15" display. Below you'll find some of the first ever images of the only prototype unit in existence which, according to Future Power employees, was built by hand.

And while the hardware specs may be slightly impressive for the \$799 that Future Power plans to market the unit at, the likes of its external casing is far from original. The E-Power prototype reeks of Apple's industrial design. From the curvy ventilation system to the circular design on the power button, and from the translucent cables to the arch shaped USB keyboard, the E-Power has "borrowed" it all. About the only thing the unit lacks is the iMac's handle.



Future Power representatives fully acknowledged their ill-practice of ripping off Apple's design work, as they responded to Apple loyalist surrounding the booth shouting phrases such as "Apple is going to sue you guys!" Representatives responded to questions about how they plan to avoid losing a lawsuit by making such statements as "You know why they can't sue us? Because there is a big difference -- our machine has a floppy. How can you make a computer without a floppy!"

Future Power employees also claimed that the E-Power mouse is not round like the iMac's, attempting to provide yet another difference in their product design. It was obvious that the folks at Future Power were intimidated by the onslaught of accusations being thrown their way by show-goers, and at times seemed overly defensive and angered.

Additionally, representatives from Future Power onhand at the PCExpo seemed to contradict themselves when asked when they plan to begin shipping units of the E-Power personal computer to customers. One representative said they would be delivering units in October or November, while another said that they hope to have the E-Power on the street by next January. Meanwhile,

product information distributed at the expo says units should be available as early as this summer, via more than 500 value added resellers.

Not surprisingly, the E-Power will be available in "five fun flavors" according to a Future Power press release -- ruby topaz, sapphire, emerald, and amethyst. The unit will also ship with a clear USB mouse. Obviously, we are not intrigued.

"This is just disgusting", one conference attendee said to a friend checking out the E-Power prototype. "I can't believe you are actually touching that thing." Others just strolled by the Future Power booth, only slowing down to grin and comment "Nice attempt."