

Mac Viruses

Well, the flu season is upon us and with all those viruses floating around I thought we should look at your Mac catching one.

"But Macs don't get viruses". Not true. All operating systems are vulnerable to getting sick including Macs. What you need to understand is Macs don't get Windows viruses and Windows PCs don't get Mac viruses. While you can't get a PC virus you are however capable of transferring one. I will be explaining and examining the basic bad stuff out there and include some advice on how to keep your Mac healthy. Sorry old timers, but this article is meant for Mac OS X. Before I get started, if you are experiencing problems with a Mac, please don't assume that is a virus. I have seen many users go out and buy Norton AntiVirus only to discover all they had was a corrupted .plist (preference file) or some other easily correctable condition.

What is a computer virus?

Actually there are several nasty things that get lumped together as "viruses". Malware, short for malicious software, is created to sneak into your computer and operate without your consent. Malware could be as simple as reporting your favorite websites to taking your computer down. Trojan horses, viruses, worms, adware, spyware, rootkits and macros fall under the category of malware.

A trojan horse or trojan comes from Greek mythology where the people of Troy rolled this huge wooden horse into their city only to later discover it was housing Greek soldiers. That is exactly what a trojan horse does. A trojan pretends to be some useful/essential plugin or a great free game when in reality, it is designed to do harmful things to your computer.

A computer virus is like a regular virus that travels from one person to another, only it spreads its bad code from one computer to another. Typically these are transferred via email, networks, Internet, USB drives, CDs, DVDs and dare I say floppy disks.

Worms differ from viruses in that they don't require attachment to a program, but just spread from the host computer.

Adware is just what it sounds like, advertisements that run on your computer after software was installed.

Just like real world spies, Spyware is meant to be hidden from the computer user and secretly monitors the users actions or even gathers personal data.

There also is commercial Spyware which is intentionally installed to covertly observe the actions of the user. Typically these are utilized to check that John is doing his work and not playing online poker.

Rootkit come from the Unix term Root which is a high level user. Rootkits are one or more programs targeted to conceal themselves from the user and undermine the operating system.

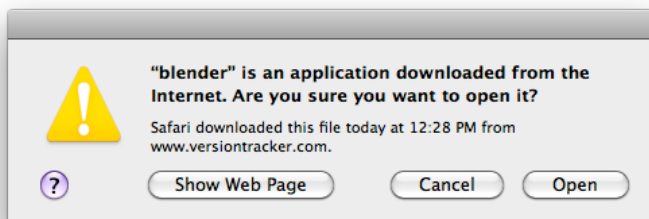
Macros take advantage of Microsoft Word's macro language which is used to automate actions, to infect your Word files.

So how vulnerable are the Macs?

Not very. The core of Apple's operating system is Unix, a very secure system that requires permission from an administration level user to make any system alterations. This is why when you update the system or install an application you will get this dialog box:



If you download an application from the web you will get this warning:



Snow Leopard takes it a step farther by warning of some types but not all of malware:



At this point in time, the weakness of the Mac mainly rests on you. If you allow a malicious program to be installed, you have lost protection.

So what malware does a Mac user have to deal with?

Trojan Horses:

There are a couple of these that are discussed, but they don't really exist "in the wild" meaning they were created as proof of concept by programmers or anti-virus companies. However trojans are where the Mac is most vulnerable.

Maybe the first was a file posted on MacRumors Forum *claiming to be the latest Leopard Mac OS X 10.5 screenshots. The file was named "latestpics.tgz" and the resultant file decompresses into what appears to be a standard JPEG icon in Mac OS X but is actually a compiled Unix executable in disguise. The file sent itself to other users in your AIM/iChat buddy list.* Note: I don't believe this one presently exists.

There is a new variant of the DNS charger trojan known as *OSX_JAHLAV.K*. The Apple-specific malware, once it makes itself at home on your computer, will redirect your Internet browser to phishing sites and malware-infected web sites. *OSX_JAHLAV.K* has a particularly nasty trick up its sleeve — it sends you to a site that advertises fake antivirus software that will notify you that you have an infection until you pay to register and have it removed.

Another, called *OSX.RSPlugA* surfaced in 2007 was spotted in the wild in 2007 being served by 65 porn sites. Visitors to any of the sites would click on a link to a "video" only to be told they didn't have the latest version of some video software, and were then presented with a link to the "upgrade." Instead of new video software and a naughty clip they got a program, which once installed changed the target machine's network settings. Among the other things the Trojan could do: If you tried to visit the Web site of your bank or credit card company, your browser session would be intercepted so that your user name and password could be captured as you typed them in.

Still another has been seen on BitTorrent file-sharing networks attached to pirated versions of Mac software like iWork and Adobe Photoshop CS4. This Trojan, known as the *iServices Trojan*, joined targeted Macs into a botnet — meaning that many compromised machines can be controlled remotely in order to carry out malicious actions as a group.

AppleScript.THT comes either as a 3.1 MB application dubbed *ASht_v06* or as a 60 KB compiled AppleScript script called *AShtv05*. Once a user downloads and runs one of those executables, their system is infected. When active, *AppleScript.THT* exploits a recently outlined Apple Remote Desktop Agent vulnerability.

Viruses, worms, adware, spyware, rootkits:

Aside from the trojans listed above being lumped in as viruses and utilitarian commercial spyware, I have not seen anything out there.

Macros:

There are lots of Microsoft macro viruses that attack Microsoft Office files on a Mac. The danger is to the files and not the Mac. The current Mac Microsoft Office 2008 does not support macros so no problem there. If you are running an older version of Mac MS Office like 2004 you are vulnerable even with the latest Mac operating systems. These can impact the Office program so even when you create a new document it will contain the virus. You can disable this capability but you still must run an antivirus. These are Office viruses not Mac or Windows viruses so they are cross platform and work on either Mac or Windows.

Other stuff:

There is a nasty virus that is floating around on the web. At this point in time it does NOT infect the Macs but that could change at any time so you should be aware. As you are on the Web a very official looking window appears and warns you that it has scanned your system and found multiple viruses, spyware, et cetera. They request you click a button to clean your computer. What really happens is that it will download and install a virus that takes over your computer and blocks any antivirus programs that you may have. Then you are forced to send them money for a program to get it off your computer. The clever thing is that it will download the virus no matter where you click on the window. It will download those files on the Mac as well but since they are .exe files they will not run on the Mac. Just go to your Downloads Folder and trash them. Whenever you see this warning window on the Web just quit your web browser and relaunch it.

So what can I do?

- 1) Only download files from reputable sites like Apple, Macupdate or Versiontracker. That free antivirus software or utility download that you discover on some obscure site may actually be a virus that unintentionally install.
- 2) Don't download illegal software or files. The bad guys know what you do, and will take advantage of it.
- 3) To lessen slip ups, create a separate User that does not have administration rights and use that for day to day use.
- 4) Install an antivirus. At this time, I don't see this as a good option. If you follow the three steps above you should be fine. Antivirus programs can be incomplete, buggy, slow and basically only offer support for known viruses and not necessarily new ones. Some options are Avast Antivirus Mac Edition, iAntiVirus, ProtectMac AntiVirus, Intego VirusBarrier X5, Symantec Norton AntiVirus, Snow Leopard Cache Cleaner and ClamXav. These vary from \$69 to shareware to free. All have some issues and some will not work with Snow Leopard. For user reviews, go to www.versiontracker.com. MobileMe does scan MobileMe email for viruses. If you need to deal with Office files that you don't create I would check out the basic ClamXav 2.0.2. It is free and will run on Snow Leopard. Obviously business environments are in greater need of an antivirus when dealing with other platforms. The computer environment is very fluid so what I have written today may be totally different tomorrow so stay as current on this issue as possible.