


A Big Mac Attack?

By Ken Dunham



Many of you have undoubtedly heard that a new Macintosh Trojan is on the loose, and that Mac users can no longer claim they are safe from viruses. Is this true? Is there a big Mac malicious code attack on the horizon for the purported complacent and/or ignorant Mac user population?

In the late 1980s and early 1990s what was one of most popular platforms for virus activity? Macintosh computers with floppy disk infectors like WDEF running wild as Mac users shared files with one another. That's right – NOT Windows, NOT Linux, but believe-it-or-not, the Macintosh operating system. The problem worsened by the early 1990s when HyperTalk script viruses designed for HyperCard emerged in the wild, which this author originally discovered.

Windows 95 soon came along, as did World Wide Web point-and-click type Internet access. An explosion of malicious codes on the Windows platform and the development of Macro viruses for Microsoft Office quickly took the stage.

In 1998 a new Macintosh worm spread like wildfire in the Macintosh community called AutoStart. Reports ran wild about the complacent Macintosh community having a serious worm threat on their hands for once. I remember this incident, as a first-responder on the scene globally, and it was a notable and significant Macintosh worm threat – the first in many years. But were the press reports correct? Would this be the start of a new era for Macintosh malicious code threats? AutoStart came and went and Mac users continued to use their computers without fear of virus attacks like those plaguing their Windows cousins.

In 2001 another interesting Macintosh threat emerged, the Simpsons Applescript virus. This, too, came and went but did not have any significant impact in the wild like AutoStart (four years earlier). It may have helped ratings, however, for the popular *Simpsons* television show?

Smaller threats like the Simpsons virus are reported every so often, constantly raising the media flag for a possible new Macintosh big bang. Some, like Renepo in 2004, are just a proof-of-concept and are not in the wild. Meanwhile analysts point out that Mac users do not have much to worry about BUT are

becoming increasingly complacent and therefore vulnerable to attack. Others claim that Macintosh users are less savvy than Windows users and are more likely to have a vulnerable computer or be tricked by social engineering.

A flurry of activity in early 2006 raised the big Mac attack flag in the media again, with the Leap worm, aka Oompa, and the Inqtana worm that spreads through an Apple BlueTooth Directory Traversal vulnerability. Later in the year iAdware surfaced, leading to additional media reports on the pending doom and gloom for Mac users facing new virus threats with quotes like, "In theory, this program could be silently installed to your user account and hooked to each application you use," according to an F-Secure blog.

By the end of 2006 comments from trusted sources like F-Secure caught the attention of the author and others. One year later a new Mac threat surfaced in the wild with limited distribution, spread on pornography websites changing DNS settings, if executed on a Macintosh computer. Debate arises on how prevalent the threat was in the wild and if it was a big deal. Some inaccurately claim it was the first Mac OSX Trojan...the media saga continues.

What does the future hold for Mac users facing possible malicious code attack? Let's attempt to take a measured look at the indicators that influence such a prediction:

1. Macintosh software contains vulnerabilities that may be exploited by malicious code. Inqtana is a good example of this type of threat in 2006.
2. Macintosh users frequently ask if they even need anti-virus software since there are no apparent prevalent or likely attacks facing their computer.
3. Macintosh users are a mixed bag of competency, with some of the most highly qualified security professionals loving the BSD and Mac OSX mix, and others enjoying the simplicity of a solid operating system designed with the consumer in mind.
4. In studies performed by the author, risky Internet behavior – like surfing for porn or cracks – increases the likelihood of a malicious code encounter or attack by as much as 90 percent.
5. The crystal ball of the media and some security professionals is, well, not so bright. Each time we hear of a threat, gloom and doom emerges somewhere – wrong each time to date.

6. The last significant and highly prevalent global Macintosh threat was the AutoStart worm family in 1998 – NINE years ago.
7. Simple population dynamics dictates, through sheer statistics, that Windows users will bear the brunt of attacks.

Are Macintosh computers and user vulnerable to attack? Yes. Will we see new Macintosh threats? Yes. Will there be a massive uprising of Macintosh threats in the near future? Highly unlikely, given the facts to date. Will a new Mac worm emerge? Possibly, but unlikely, given facts to date. Will criminals increasingly target Macintosh computers for exploitation and profit? Yes, as assets avail themselves and criminals mature their operations.

In the end Mac users have the same responsibility that all other computer users have: practice safe computing. Each computer has a certain amount of risk associated with it, especially computers with the Windows operating system, given the large volume and variation of attacks matured on the platform to date.

So then, what do you want for Christmas? Forget about media hysteria and go with the facts. I wonder if a PowerBook can fit into that knitted stocking above the fireplace...

About the Author

Ken Dunham, CISSP, GREM, GSEC, GCIH Gold Honors, GCFA, Senior Engineer, Director of Global Response for iSight Partners, can be reached at ken@kendunham.org.