

Don't Assume Your Macs Are Immune to Security Flaws

Martin Reynolds

The growing number of Macintosh security flaws won't affect most enterprises. But businesses using Macs must guard against malicious-code attacks and spyware infestations.

NEWS ANALYSIS

Event

On 21 March 2005, Symantec, a provider of antivirus and other security software, released a report stating that it has identified an increasing number of vulnerabilities in the current version of Apple Computer's Macintosh operating system (Mac OS X). Symantec reported that it had identified 37 high-impact Mac OS X vulnerabilities in the preceding year. Apple offers security updates and information on many of these vulnerabilities at www.apple.com/security/ and www.apple.com/support/security/.

Analysis

The enterprise impact of the growing number of identified Mac OS security flaws will largely be limited to businesses — such as those in the news media and the visual arts — that rely on the Mac. The Macintosh installed base is relatively small, with only about 3 percent of systems in use today running the Mac OS. Therefore, if an infected Macintosh attempts to spread a worm, it will reach a system resistant to that infection 97 percent of the time. A hybrid worm targeting both the Mac OS and Microsoft Windows could be developed, but such an attack would be difficult to orchestrate. The Mac OS is also a harder target, partly because open-source code and limited hardware diversity mean that vulnerabilities can be quickly detected and patched with less risk to applications. However, it only takes one exploited weakness to cause trouble.

Enterprises using the Mac OS should be more concerned about the risk of these vulnerabilities being exploited by individual hackers attempting to steal sensitive information. Another potential problem is spyware. Although it is almost nonexistent on the Mac platform today, problem spyware could emerge. Spyware that exploits vulnerabilities can establish itself more deeply in the system, becoming both harder to detect and harder to remove.

Recommendations for enterprises using the Macintosh operating system: Don't assume that your Macintosh systems are immune from viruses and other malicious-code attacks. Ensure that proper perimeter firewall and filtering protection is in place, and guard against spyware infestations.

Analytical Source: Martin Reynolds, Gartner Research

Recommended Reading and Related Research

- "Preventing and Removing Spyware" — Removing spyware is an inexact process that requires multiple methods, both simple and complex. **By John Pescatore and John Girard**
- "Diversity Increases Security in Desktop Computing" — In enterprise computing, as in nature, a diverse environment is more resistant to infection. **By Ray Wagner and John Pescatore**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509