



Topics

News

In Depth

Reviews

Blogs

Opinion

Shark Tank

IT Jobs

White Papers

Webcasts

Security

More

[App Security](#) | [Business Continuity](#) | [Cybercrime and Hacking](#) | [DRM and Legal Issues](#) | [Data Security](#) | [Malware and Vulnerabilities](#) | [Privacy](#) | [Security Hardware and Software](#)

[Home](#) > [Security](#) > [Security Hardware and Software](#)

News

## Apple admits Mac scareware infections, promises cleaning tool

After taking heat for not helping users, Apple takes major step by owning up security problems in Mac OS, says expert

By Gregg Keizer

May 24, 2011 09:38 PM ET

[Comments \(0\)](#)[Recommended \(7\)](#)

Computerworld - Apple on Tuesday promised an update for Mac OS X that will find and delete the MacDefender fake security software, and warn still-unaffected users when they download the bogus program.

The announcement -- part of a [new support document](#) that the company posted late Tuesday -- was the company's first public recognition of the threat posed by what [security](#) experts call "scareware" or "rogueware."

"In the coming days, [Apple](#) will deliver a Mac OS X software update that will automatically find and remove Mac Defender malware and its known variants," Apple said in the document. "The update will also help protect users by providing an explicit warning if they download this malware."

Apple also outlined steps that users with infected Macs can take to remove the scareware.

### Apple Watch

[Apple admits Mac scareware infections, promises cleaning tool](#)

[Apple to Lodsys: 'App makers are protected by \[our\] license'](#)

[Mac App Store's slow updates expose users to security risks](#)

[A tale of two Apple Stores \(the first two\)](#)

[Independent Mac retailers emerge from the Apple Store shadow](#)

[Apple to refresh MacBook Air in June or July, says report](#)

[Next iPhone's A5 CPU: Enough reason to upgrade?](#)

[Analysts split on iPhone over-the-air-update buzz](#)

[Apple's iMac, MacBook Pro lines are SSD friendly](#)

[Apple releases iOS 4.3.3 to patch location bugs](#)

Andrew Storms, director of security operations with nCircle Security, was surprised that Apple said it would embed a malware cleaning tool in Mac OS X.

"That's new ground for Apple," Storms said, pointing out that the move is a first for the company, which until now has only offered a [bare-bones malware detection mechanism](#) in Mac OS X 10.6, aka Snow Leopard, and then only populated it with a handful of signatures.

"Not only is Apple going to help customers remove [Mac Defender], but by doing so, they're also admitting that there are security problems with Mac OS," Storms said.

MacDefender -- which also goes by names such as MacProtector and MacSecurity -- first [popped up earlier this month](#) when French security company Intego said it had found the scareware in the wild.

Apple admits Mac scareware infections, promises cleaning tool - Computerworld  
Scareware and rogware are terms for bogus security software that claims a personal computer is heavily infected with worms, [viruses](#) and other malware. Once installed, such software nags users with pervasive pop-ups and fake alerts until they fork over a fee to purchase the worthless program.

MacDefender was the first piece of professional-looking scareware to target Macs.

Last week, [Microsoft](#) said it had found evidence in MacDefender that the fake program was created by the same group responsible for a [fast-growing scareware family aimed at Windows users](#).

"That shouldn't have surprised anyone," Storms said today. "Why should the hackers reinvent the wheel?"

Apple has taken criticism for not publicly responding to the MacDefender threat.

In several posts over the last week, ZDNet blogger Ed Bott -- who usually covers Microsoft and Windows topics -- laid out information he had received from insiders at Apple support.

Those tech support representatives told Bott, and provided documents, that said Apple had told them [not to help Mac users](#) who had been duped into downloading and installing MacDefender.

Both Intego and U.K.-based Sophos have used the information Bott has published and his estimates of the number of Macs infected to also take Apple to task.

"Apple's famous PR savvy apparently doesn't apply to handling security incidents," Chet Wisniewski, a Sophos security researcher, said in a post on his company's blog on Tuesday. "It is genuinely tragic that such a large number of OS X users are falling victim to this scam, and Apple's response is less than helpful."

Intego sells Mac-specific security software, and Sophos offers a free Mac antivirus program.

"What this shows is that nobody is safe," Storms said. "The truth is that the vast majority of malware isn't on the Mac, it's not on the [iPhone](#), it's specifically on Windows."

"I say that's because of Windows market share, but Mac users have long claimed that it's because Mac OS is more secure, or Mac users are more intelligent and don't fall for these ruses," he said. "Well, guess what, this proves the point that it doesn't matter what OS you're using. In the end, it all depends on the user to understand what's malware and what's not."

**Gregg Keizer** covers Microsoft, security issues, Apple, Web browsers and general technology breaking news for Computerworld. Follow Gregg on Twitter at [@gkeizer](#) or subscribe to [Gregg's RSS feed](#) . His e-mail address is [gkeizer@computerworld.com](mailto:gkeizer@computerworld.com).

[Read more about Security Hardware and Software](#) in Computerworld's Security Hardware and Software Topic Center.

---

[Comments \(0\)](#) | [Add yours](#)   [Recommended \(7\)](#)   [Print](#)