OS X Trojan Horse Is a Nag

By Leander Kahney

Story location: http://www.wired.com/news/mac/0,2125,63000,00.html

12:44 PM Apr. 09, 2004 PT

(Editor's note: This story corrects an earlier report that stated that the Macintosh operating system had become a target of a malicious Trojan Horse.)

Security experts on Friday slammed security firm Intego for exaggerating the threat of what the company identified as the first Trojan for Mac OS X.

On Thursday, Intego issued a press release saying it had found OS X's first Trojan Horse, a piece of malware called MP3Concept or MP3Virus.Gen that appears to be an MP3 file. If double-clicked and launched in the Finder, the Trojan accesses certain system files, the company claimed.

While Intego said the Trojan was benign, it said future versions could be authored to delete files or hijack infected machines. In the release, and in subsequent telephone interviews, Intego was vague about the purported Trojan's workings and its origins.

On Friday, Mac programmers and security experts accused the company of exaggerating the threat to sell its security software.

"They gave the impression that this is a threat, but it isn't," said Dave Schroeder, a systems engineer with the University of Wisconsin. "It is a benign proof of concept that was posted to a newsgroup. It isn't in the wild, and can't be spread in the wild. It's a non-issue."

"They are spreading FUD to sell their software," said Ryan Kaldari, a programmer from Nashville, Tennessee, referring to the shorthand for fear, uncertainty and doubt.

Rob Rosenberger of Vmyths said he'd seen virus hype many, many times, and if antivirus companies put out alarmist press releases, it's for one of two reasons: "Either they're delusional or they're trying to own the hysteria," he said. "This has been going on for 16 years now."

Rachel Keiserman, a tech-support person at Intego, denied on Friday that her company exaggerated the threat or was attempting a publicity stunt. "It's not a hoax or anything like that." She declined to comment further and pointed to a press release listing questions and answers, which defended the company's decision to classify the issue as a threat.

"While the first versions of this Trojan Horse that Intego has isolated are benign, this technique opens the door to more serious risks," the company said. "The exploit that it uses is both insidious and dangerous, and it is our duty as a vendor of Macintosh security solutions to protect our users. We don't believe in waiting until the damage occurs, unlike some of our competitors."

Technically, the threat isn't a Trojan Horse by the standard definition: It isn't a working piece of malicious code and can't easily be spread to other computers, experts said. Instead, it is a demonstration of a possible threat.

"We're talking about theoreticals here," said Schroeder. "It *is* possible for OS X to be infested with Trojans, viruses and security issues, but until it is, they aren't justified in raising the alarm."

The demonstration contains a real MP3 file of someone laughing. When launched in jukebox software like iTunes, the MP3 file plays and nothing else happens. But if double-clicked in the Finder, the MP3 file plays and a warning is displayed.

The program can't be spread by e-mail or through a file-sharing network unless it is compressed using software like Aladdin's Stuffit. Failing to compress the MP3 file before sending it renders the software inoperative.

The program exploits a vulnerability that goes back to the original Mac operating system: The system allows programs to appear as a file. Programs can have any icons, names or file extension. In other words, users could be tricked into activating a malicious program, thinking they were opening a document, picture or song.

The vulnerability was exploited several times by Trojans authored for previous versions of the Mac OS.

Mac programmer Bo Lindbergh wrote the threat demonstration and posted a link on the comp.sys.mac.programmer.misc newsgroup on March 20. The link leads to a site in Sweden. The file has now been removed. Lindbergh didn't respond to an e-mail requesting comment.

Symantec on Friday said it was aware of the software. "It is a proof-of-concept Trojan that does affect the Mac platform; however, it is currently not present in the wild," the company said in a statement. It said it would continue to monitor the situation.

Likewise, Apple spokeswoman Natalie Sequeira said the company was investigating. "We are aware of the potential issue identified by Intego and are working proactively to investigate it," she said.