

Bluetooth worm targets Mac OS X (Fixed in 10.3.9 Security Update, 10.4.1)

Just a day after experts warned of what is believed to be the first Trojan in the wild to target Apple Computer's Mac OS X, alerts are being published on a new worm that exploits an 8-month-old vulnerability in the operating system.

The new Inqtana worm spreads through a security flaw in Apple's Bluetooth software, antivirus vendors Symantec and F-Secure said on Friday. Apple provided a fix for the flaw last June with security update 2005-006.

The worm attempts to use Bluetooth to propagate. Once it infects a computer it searches for other Bluetooth-enabled devices and sends itself to those it finds, Symantec said.

Inqtana is a "proof-of-concept" worm, according to Symantec and F-Secure, meaning it's an example of attack code, but itself likely won't affect many users, if any at all. Inqtana is not believed to have actually attacked Mac users. Furthermore, it uses a Bluetooth component that is locked to a specific address and expires next week, according to F-Secure.

"It is quite unlikely that Inqtana would be any kind of threat," F-Secure said on its blog.

However, two examples of malicious software to target Mac OS X in two days may be the start of a trend, Vincent Weafer, senior director at Symantec Security Response, said in a statement.

"We have speculated that attackers would turn their attention to other platforms, and two back-to-back examples of malicious code targeting Macintosh OS X this week illustrates this emerging trend," he said. "While this particular worm is not fully functional, the source code could be easily modified by a future attacker to do damage."

The new worm follows the Leap Trojan that was discovered Thursday. Symantec says it believes the two pests were developed on a parallel time line and that Inqtana was not created in response to Leap.

Symantec recommends that Mac OS X users keep antivirus and firewall software, as well as operating systems, up to date. Apple has a safety guide on its Web site