

Archive

MS Windows Source Code Leak Could Spell Trouble for Microsoft

October 30, 2009 06:35 AM

Officials at Microsoft Corporation - the world's largest software maker - confirmed late last week that segments of the confidential source code underlying the popular Windows operating system have been leaked onto the Internet. The leak was relatively small, little more than one percent of the hundreds of millions of lines of instructions that make up the complex software. But Windows is the world's most widely-used operating system, running on about 90 percent of all personal computers. The leak could threaten Windows' reliability and its dominance of the market.

Federal law enforcement agents are investigating the details surrounding the Windows source code leak. But computer users are probably going to be less concerned about nabbing the culprit than about the potential damage the leak might cause to their favorite operating system. Although most of the leaked source code appears to be the basis for the older Windows NT 4.0 and Windows 2000 operating systems, Microsoft's Windows XP and many of its other new software products are also based on some of that older source code. And while only about 600 megabytes about one CD-ROM's worth, of the Windows instructions were revealed in the leak, that still represents roughly 13 million lines of code.

Many computer security experts believe that 13 million lines would give virus writers plenty to work with to create new threats to Windows-based computers. Martin Roesch is the chief technology officer for Sourcefire, a firm that specializes in detecting intrusions to computer systems.

"There's certainly a good chance that there's going to be some software in there that people figure out is still in widespread use," he said. "With as much code as we're talking about here, there's a definitely a pretty good chance that there's going to be some near-term attacks that result from this."

In fact, within four days of the code leak, a new vulnerability was discovered in Internet Explorer 5, an older version of Microsoft's popular web browsing software that comes bundled with Windows. The vulnerability won't impact newer versions of the browser.

Some computer security experts have played down the significance of the code leak. After all, they point out, many of the viruses that attack Windows - and there have been many - of them were designed prior to the source code leak. And Bob Fleck, Director of Security Services at Secure Software, notes that many people outside Microsoft were already familiar with a good portion of the Windows source code.

"That's because Microsoft already has an initiative called the Shared Source Initiative, where universities, partners and other governments have access to the source code for doing their security research," said Bob Fleck. "A lot of people can already see this stuff."

Microsoft's Shared Source Initiative appears to be at least partly to blame for the leak. The program allows trusted organizations such as government agencies, universities and private companies to gain access to selected parts of Microsoft source code that they need for research and product development. The code is released under strict guidelines that limit how the information can be used. Despite the serious legal consequences for anyone leaking the confidential source code, many industry experts say they're surprised that the leak didn't occur sooner.

In addition to the millions of computer users concerned about security after the leak, Microsoft itself has reason to be concerned. The company's intellectual

property is being distributed without its permission and outside its control. While it is highly unlikely that 1.5 percent of the source code could form the basis of a competing version of the Windows operating system, some of that code could still be of use to Microsoft's competitors. It might enable them to make software designed to run in Windows work better on competing operating systems.

The question of whether it is legal to make any use of the liberated code - even read it - has sparked a debate among programmers and legal scholars. Bob Fleck echoes the concerns of many programmers who contribute to the free open source operating system, Linux.

"Everything I've seen so far in comments from people in the open source community has indicated that they're being very wary and saying, 'Nobody look at this.' This could have very bad repercussions if we're seen to be looking through Microsoft source code in order to get ideas," he said. "A developer who was known to have looked through Microsoft source code, in particular this leaked source code, could have a negative legal impact on projects they worked on in the future."

Some Linux programmers are already under legal attack, for alleged copyright infringement. SCO Group, a private software company, claims that significant portions of its UNIX source code were introduced into Linux without the company's permission. Linux advocates and users fear similar lawsuits from Microsoft could be brought to trial if portions of the leaked Windows code somehow turn up in new versions of Linux.

But Christine Farley, an associate professor of law at American University in Washington, DC, says the leaked Microsoft source code may not be as dangerous for developers to see as some believe.

"Why Microsoft people would be in a tizzy right now, is that if this is being widely distributed and it seems that it is, they might lose their trade secrets

protection in the source code," she explained. "So this is something like a significant portion of Coke's formula for their Coca-Cola being distributed over the Internet. Once a trade secret is no longer secret, it's no longer intellectual property that you can protect under the law."

The source code leak might not be all bad news for Microsoft. Some industry analysts have predicted that users of older Windows operating systems might be persuaded to upgrade to the company's latest products to minimize their security risk. But others predict that Windows users might be more willing now to switch to alternate operating systems such as Linux or Apple's Mac OS-X. If they perceive the risks of using Windows outweigh the hassles of buying new software or even new computers, many users could find making the switch away from Windows has become a whole lot easier.