The Highly Reliable Times   Mic

LATEST UPDATES: NCsoft WON'T PLAY WITH LINUX · WINDOW

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

P2P Networks Turn Up Sensitive Corporate, Government Documents

A House committee hearing shows that the security dangers of file sharing over peer-to-peer networks is still a major problem.

By Larry Greenemeier, InformationWeek
July 25, 2007
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=201200981

The House Oversight and Government Reform committee thought a hearing it held four years ago about the security dangers of file sharing over peer-to-peer networks had sufficiently addressed the problem. Clearly it hadn't. The committee convened a follow-up hearing Tuesday after an informal investigation into P2P security recently turned up files containing the corporate strategies of Fortune 500 companies, military operation orders, and other sensitive information.

The committee had a strong interest in "national security and leaks bubbling out of the government," Eric Johnson, director of Dartmouth's Glassmeyer/McNamee Center for Digital Strategies and a professor of operations management at Dartmouth's Tuck School of Business, told *InformationWeek* after testifying before the committee Tuesday.

Some members of the committee want to crush P2P file sharing out of existence, "but that game has been played and there are only two large players left in North America," Johnson said, referring to LimeWire and Morpheus. "Most of the others come from outside the U.S., so shutting them down is not a really viable approach."

The primary outcome of the hearing is that committee members are starting to better understand the security risks that arise when government and business workers engage in file sharing from computers that contain sensitive information. "Today's hearing was one of saying, look, this problem has been around for a few years and it's getting worse," Johnson said. "There are a lot of government and corporate documents leaking out, and we need to do something."

Committee members know this first hand. Using the LimeWire P2P program, committee staffers ran a series of basic searches prior to Tuesday's hearing. "What we found was astonishing: personal bank records and tax forms, attorney-client communications, the corporate strategies of Fortune 500 companies, confidential corporate accounting documents, internal documents from political campaigns, government emergency response plans, and even military operation orders," committee chairman Rep. Henry Waxman, D-Ca., said to open the hearing. "All these files were found in unpublished, Microsoft Word document format. All were found in limited searches over the past month. It is truly chilling to

think of what private information an organized operation or a foreign government could acquire with additional resources."

Robert Boback, CEO of Tiversa Inc., which provides technology for monitoring P2P networks, testified Tuesday that his company has come across numerous sensitive documents freely available through P2P networks. This includes a corporate disclosure by an attorney whose clients are the world's largest pharmaceuticals manufacturers. The document "disclosed 436 sensitive and confidential files related to those clients," Boback said. This information included pending litigation.

One of the documents Tiversa found, dated April 2007, labeled "confidential," and addressed to Waxman and the committee's ranking member Rep. Tom Davis, R-Va., "appears to address questions regarding drug trials" of a particular pharmaceutical company, Boback said, adding, this is a "clear example of extended enterprise risk."

One of the problems with controlling P2P networks is that it's hard for many people to understand how it works, Johnson said. "So getting clear in their minds what it is and why it's a threat was one of the more successful outcomes of today." Johnson speculates that, as the government comes to better understand this issue it will enforce existing restrictions against putting government data on personal computers, particularly those accessible via P2P networks.

The Highly Reliable Times   Mic

LATEST UPDATES: NCsoft WON'T PLAY WITH LINUX · WINDOW