

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9132571&intsrc=news_ts_head

Update: Strike Fighter data was leaked on P2P network in 2005, security expert says

The information involved terabytes of data on the Pentagon's Joint Strike Fighter aircraft

By Jaikumar Vijayan

May 5, 2009 (Computerworld) Data on the Pentagon's Joint Strike Fighter aircraft that was [recently reported as being illegally accessed](#) by foreign cyberspies has been available for more than four years on a peer-to-peer file-sharing network, the CEO of a software vendor said at a legislative hearing today.

The Wall Street Journal last month reported that hackers -- possibly based in China -- had broken into U.S. Department of Defense computers and downloaded terabytes of data containing design information about the \$300 billion stealth fighter currently under development.

But Robert Boback, CEO of Tiversa Inc., a Cranberry Township, Pa.-based P2P monitoring services provider, said the company discovered the data on a file-sharing peer-to-peer network in January 2005 and reported it to the Defense Department and other federal authorities at that time.

The Defense Department could not immediately be reached for comment.

Boback was testifying at a hearing held today by a subcommittee of the House Committee on Energy and Commerce headed by U.S. Rep. Henry Waxman (D-Calif.) to discuss two new bills, one of which relates to P2P file sharing.

According to a company spokesman, the data on the Joint Strike Fighter was leaked from computers belonging to a defense contractor. At that point, the data was "not seen in China" but was disclosed from computers located in the state of Georgia and another computer in Ireland, the spokesman said via e-mail.

It was not immediately clear whether the data that was being referenced at the hearing today was the same data that the *Journal* reported as being stolen. According to the *Journal*, the compromised files were related to the design of the Joint Strike Fighter and its electronics systems and could be used to help defend against the jet. However, no sensitive files were compromised in the DOD break-in, according to the *Journal*.

The intrusions that were reported by the *Journal* were believed to date back to 2007. Boback's testimony makes it clear that data on the Joint Strike Fighter project has been available for at least two years before that.

This is not the first time Boback's company has reported discovering sensitive and confidential information on P2P networks. In March, Tiversa disclosed that it had [discovered data about the communications, navigation and management electronics on Marine One](#), the helicopter now used by President Barack Obama, in a publicly available shared folder on a computer in Tehran, Iran. The data was apparently being accidentally leaked over a peer-to-peer file sharing network last summer, according to the company.

Two years ago, at a similar legislative hearing, Boback testified about how his company had discovered [millions of documents, both governmental and private](#), containing sensitive and sometimes classified information on file-sharing networks after being inadvertently exposed by individuals downloading P2P software on their computers.

The documents Boback said his company had discovered at that time included the Pentagon's entire secret backbone network infrastructure diagram, complete with IP addresses and password change scripts, and contractor data on radio frequency manipulation to beat improvised explosive devices (IED) in Iraq.

Over the past 60-days alone, Tiversa uncovered nearly a million instances where computers were leaking sensitive data on P2P networks, Boback told members of the House committee today.

Most often associated with illegal music sharing, P2P software tools are widely used to share media and data files between Internet-connected computers. If the software is not properly configured on a system, a user could end up [exposing the entire contents of their hard disk](#) to other users of P2P networks.

The issue has been a well documented and understood for several years now, but data leakage on P2P networks continues to be a widespread problem. The issue has been worsened by what is seen by some as a tendency by the [distributors of popular P2P file-sharing programs](#) such as Kazaa, LimeWire and Morpheus to include features that heighten the risk of such inadvertent exposure.

One of the bills discussed at today's hearing is aimed at getting developers of P2P software to make it harder for users to inadvertently expose sensitive data while exchanging media files over file sharing networks.

The bill, called the [Informed P2P User Act \(HR 1319\)](#), was introduced in March by Rep. Bono Mack (R-Calif.) It requires P2P software makers to provide clear notice to users about how file-sharing software could allow all files on a computer to be searched and copied by others and to obtain informed consent from users before installation. The bill would also require P2P software developers to make it easier for users to uninstall the software if needed.

David Sohn, a senior policy counsel at the Center for Democracy and Technology (CDT) who testified at today's hearing, called the bill a good idea. "CDT absolutely supports the principle that file-sharing software should clearly communicate" how a user's files may become available to third parties, he said.