

The Washington Post

Soldiers' Data Still Being Downloaded Overseas, Firm Says

Sensitive Information Found by Using 'Peer to Peer' File-Sharing Software

By Ellen Nakashima
Washington Post Staff Writer
Friday, October 2, 2009

The personal data of tens of thousands of U.S. soldiers -- including those in the Special Forces -- continue to be downloaded by unauthorized computer users in countries such as China and Pakistan, despite Army assurances that it would try to fix the problem, according to a private firm that monitors cybersecurity.

Tiversa, which scours the Internet for sensitive data, discovered the data breaches while conducting research for private clients. The company found, as recently as this week, documents containing Social Security numbers, blood types, cellphone numbers, e-mail addresses, and the names of soldiers' spouses and children.

The availability of such data, security experts say, exacerbates the threat of identity theft and retaliation against troops on sensitive missions. In addition to using the information to drain financial accounts, hackers could pose as soldiers in an effort to ferret out sensitive data, including passwords to government systems.

Such disclosures represent a "major security risk" to the service members and the military, said Rep. Edolphus Towns (D-N.Y.), chairman of the House Oversight and Government Reform Committee, which was informed of the data breach by Tiversa.

The company found the sensitive documents by using "peer to peer" file-sharing software, which can be easily downloaded on the Internet and which allows computer users to share music or other files. While such software is popular -- in any given second, about 22 million people are on file-sharing networks -- many computer users do not realize that it can make the contents of their computers available to other file-sharers.

Towns, who is drafting legislation to address the problems raised by peer-to-peer technology, said: "What is striking about these file-sharing leaks is that these aren't one-time events. Once this software is installed and files are leaked, the leaking is continuous."

In 2003, the Army instituted policies barring the unauthorized use of peer-to-peer software. The Pentagon did the same in 2004, and defense contractors have followed suit. But critics say policies often are not enforced.

Of particular concern to security experts is Tiversa's discovery of personal information about soldiers in the 3rd Special Forces Group (Airborne), whose mission area is Africa.

"These guys are operating behind lines, and they are absolutely in the deepest part of the fight," said James Mulvenon, vice president of the intelligence division at Defense Group, a security consulting firm. "The fact that the documents have the names and addresses of the families and all the pressures that could be put to bear on them, it's a nightmare."

Carol Darby, a spokeswoman for the Army Special Operations Command, confirmed the data breach but described it as an isolated incident. She said those involved in the breach had been punished, but she did not provide details.

"The unit now has measures in place to reduce the chances of this happening again," she said.

Robert Boback, chief executive of Tiversa, said such precautions are not sufficient safeguards.

"Every company, agency and defense contractor will say that they have a policy against P2P on company-owned equipment and blocking, usually through intrusion detection," he said. "The fact remains that these documents are still going out."

Tiversa saw the Special Forces data on servers in Pakistan in May and immediately notified military criminal investigators. Similarly, in April 2008, the firm spotted spreadsheets from Army master sergeants' promotion lists containing the personal data of 60,000 soldiers, as well as data on several thousand civilians and soldiers from the 1st Signal Brigade. All have been downloaded recently in foreign countries, Boback said.

In October, the secretary of the Army assured then-Sen. Joseph R. Biden Jr., who was concerned about the breach, that the Army would alert the soldiers, try to have the information removed from an unauthorized host site, and better educate the Army workforce on preventing breaches of personal data.

Gary Tallman, an Army spokesman, said it is "troubling" that personal information continues to appear on file-sharing networks. "Clearly there've been instances where the checks and balances have not worked and the data have gotten out. When it does happen, it's taken very seriously and we try to prevent it from happening again."

Steven Shirley, head of the Defense Department's Cyber Crime Center, said that "even very tech-

savvy organizations -- DOD and contractors -- have issues with peer-to-peer applications." Towns's committee found, for instance, that contractor documents on major weapons programs such as the F-35 Joint Strike Fighter have found their way onto these networks and have been accessed by computer users in China and other countries.

Some of these documents, while not marked "classified," are restricted under the Arms Export Control Act of 1976, or the International Traffic in Arms Regulations (ITAR), which prohibit release of the information to unauthorized foreigners. Violation of ITAR can result in a fine of up to \$1 million or 10 years in prison or both, and a civil penalty of up to \$500,000 for each violation.

Industry has long complained that ITAR is too broad.

Jeffery Adams, a spokesman for Lockheed Martin, which is building the Air Force's Joint Strike Fighter, said the company is "aware of the vulnerabilities peer-to-peer networks present to the corporation," and so prohibits employees from using such networks on company systems. He declined to comment on the F-35 documents.

Staff writer Brian Krebs and staff researcher Eddy Palanzo contributed to this report.

<http://www.washingtonpost.com/wp-dyn/content/article/2009/10/01/AR2009100104947.html>