Peer-to-Peer Threat and Actions Being Taken by Other Government Agencies

There are numerous documented incidents where peer-to-peer (P2P) software was exploited to obtain sensitive and classified government and commercial sector information when it was installed on government, private industry, or home computers. In June 2007, Pfizer reported that personal information of 17,000 employees was exposed through unauthorized P2P file-sharing software installed on a laptop, with 15,700 of these records subsequently accessed and copied by an unknown number of individuals.

P2P can also make it easier for computer viruses and other malicious software to be installed on your computer without your knowledge. According to the Department of Homeland Security (DHS), United States Computer Emergency Readiness Team (US-CERT), when P2P applications are used, it is difficult, if not impossible, to verify that the source of the files is trustworthy. These applications are often used by attackers to transmit malicious code. Attackers may incorporate spyware, viruses, Trojan horses, or worms into the files. When the files are downloaded, the computer becomes infected. By late spring 2005, DHS reported that government employees using file-sharing programs had repeatedly compromised national and military security by "sharing" files containing sensitive or classified data.

Another example of malicious use of P2P software includes Botnet cyber crimes. "Botnet" is derived from the idea of a "ro**bot net**work." Botnets refer to networks of computers that are able to be remotely controlled by outside sources. Using P2P software to surreptitiously access someone's computer, an attacker usually gains control by infecting the computer with a virus or other malicious code. In many instances, the computer continues to operate normally, and the owner is unaware that the computer has been compromised. Frequently, botnets are used to steal password and login data, bank account information, and other sensitive and personal data, but botnets could be used to access home computers of NRC staff to steal sensitive unclassified non-safeguards information being processed or stored on the home computer.

On July 24, 2007, the U.S. House of Representatives, Committee on Oversight and Government Reform, heard key testimony by government and industry experts who showed overwhelming agreement about the threat of inadvertent file-sharing over P2P networks. The following is an excerpt of the testimony showing some of the types of documents obtained by Tiversa.

Inadvertent shared information is not limited to classified information. A diverse amount of information exists across government agencies and contractors. Here are some examples:

- A document illustrating over 100 individual soldiers' names and Social Security numbers
- Physical threat assessments for multiple cites such as Philadelphia, St. Louis, and Miami
- A government contractor exposing an Air Force base physical security attack assessment
- A document titled "NSA Security Handbook"
- A detailed report from a well-known government contractor for the National Security Agency (NSA) which outlines how to connect two secure DoD networks

- Numerous Department of Defense Directives (DoDD's) on various Information Security topics
- Various Department of Defense Information Security system audits, reviews, procedures, etc. (e.g., retina scanner equipment audit, penetration detection software/equipment reviews)
- Numerous "Field Security Operations" documents, including router checklists procedures, "Network Infrastructure Security Checklist", etc.
- Numerous presentations for Armed Forces leadership on various Information Security topics, including how to profile "hackers" and potential internal information leakers
- Large numbers of Army documents marked "For Official Use Only"

While Congress investigates P2P, other government agencies are already taking action to protect their information from P2P software.

- The Department of Veterans Affairs has prohibited the use of P2P.

- Department of Transportation (DOT) users are not authorized to install or use P2P software applications unless expressly authorized in writing by the Department's Chief Information Officer. DOT cannot restrict P2P on personal computers; however, their policy prohibits employees from using or accessing DOT information if P2P software is installed or suspected of being installed on an employee's personal computer. The problem with this approach is that employees may not know they have P2P software installed on their computers because it can be inadvertently or unknowingly downloaded by other family members.

- DHS has updated its Rules of Behavior in the DHS Handbook to include the prohibition of P2P file-sharing or software. In addition, the DHS's proposed approach to sensitive data in telework situations is: (1) without prior approval from security, sensitive data cannot be stored on non-DHS computers; (2) staff must use Virtual Private Network from a DHS laptop only; (3) when using Outlook Web Access from a personal computer, do not open any Sensitive But Unclassified or For Official Use Only (FOUO) documents locally; (4) always secure a DHS laptop in case of theft or break in; and (5) do not print or store sensitive information at home.

- Department of Energy's (DOE) P2P Networking Guidance states, "P2P applications are not to be used on DOE systems that contain or process Sensitive Unclassified Information (SUI). The default condition is that no P2P technology or services are to be used except under conditions prescribed by Senior DOE Management in their Program Cyber Security Plans."