Computer Crime Investigative Unit

U.S. Army Criminal Investigation Command

Cyber Crime Alert Notice

2CAN 0028-09-CID221-9H

28 May 2009

P2P Might Leave You up a Tree

Overview:

Peer-to-Peer (also known as P2P) was dreamed up in the 1960s as pure technological possibility. In its most basic form, two computers trade information on equal footing, neither is client or server. This technology was realized in the 1980s and became an application for everyday computer users in the 1990s. As we entered the new millennium, P2P was thrust into the public eye by the precipitous rise of Napster and its equally precipitous fall. Today there are more P2P networks than keys on your keyboard and they are being utilized by millions of people worldwide. Just how prevalent are P2P networks at present? Ipoque, a European Internet analysis firm, conducted its annual study of 1.1 million users from Eight regions, including Europe, the Middle East, and the Americas. For the third year running, P2P networks produced much more traffic than any other activity on the Internet. In most cases, over half of a region's Internet traffic was P2P. P2P is technologically elegant, massively redundant, and like no other tool, allows people the world over to share information, arguably bringing us closer together. Now for the bad news…

Not everything that happens on P2P networks is completely legitimate or lawful. Most of us are familiar with at least one portion of the darker side of P2P, such as copyright infringement, which caused trouble and litigation for Napster. In that case, millions of users downloaded copyrighted songs, movies, and software without paying for them, also known as digital piracy. Unfortunately, there is more bad news. P2P networks can also be used to spread malicious software (malware), control that malware, and (perhaps most frightening to all of us) expose our personal files to millions. This is commonly known as "Data Leakage", stemming from the understanding that the distribution of sensitive data is largely unintentional. The U.S. Congress was concerned enough about the threat of data leakage over P2P that it held hearings on the subject three times since 2003. What can be found on P2P networks besides pirated music: Your bank statements, your tax return, your professional evaluations, your medical records, your pay slips, your entire Enlisted or Officer Record Brief, and sometimes even your unit's complete personnel roster, with dates of birth, home addresses, and Social Security Numbers. Worried yet? You should be.

CID elements are encouraged to brief supported installations and units on the contents of this 2CAN.

Those Leaky Peer-to-Peer Applications:

Most users install P2P applications on their home computers with the same level of concern as they would assign to installing a popular game. The danger here is that running a P2P application at home is much more like running a file sharing server than a game. But an improperly configured file sharing server could be sharing your computer's entire hard drive with millions. Remember, even if you know what you are doing when it comes to P2P, another user (your spouse, children, or friend) could make unsafe changes without your knowledge.

Contact Information:

Cyber Criminal Intelligence Program
9805 Lowen Road, Building 193
Fort Belvoir, Virginia 22060-5598

Phone: 703.805.3499 (DSN 655)
Fax: 703.805.2351 (DSN 655)
E-mail:
cybercrimintel.cciu@us.army.mil

CCIU Web Page:
www.cid.army.mil/cciu.htm

CID Cyber Lookout
On Point for the Army

Distribution:
This document is authorized for wide release with no restrictions.

"Do What Has To Be Done"

CCIU recently reviewed five popular P2P applications (i.e., Limewire version 5.1.2, BearShare version 7.1, Ares version 2.1.1.3035, eMule version 0.49c and Frostwire version 4.17.2) and found the following:

- Only Ares specifically informs the user of the threat of inadvertent data leakage over P2P networks.

- Only Limewire (by default) will not allow the sharing of documents via its P2P application; however, document sharing can be enabled easily.

- Only Frostwire warns / notifies the user when folders are shared that pose a security risk, such as the “My Documents” folder.

- In Limewire, BearShare, Ares and eMule, the entire contents of the computer system’s hard drive could be shared with relative ease and without warning / notification by the application that the user had made this ill-advised change.

WHAT’S OUT THERE FLOATING AROUND:

There have been a few recent high-profile leaks of sensitive information via P2P networks, including the technical schematics of the “Marine One” presidential transport helicopter. Working with various sources, CCIU was able to verify that other entities interested in inadvertent P2P disclosure had identified and recovered hundreds of documents of operational significance to the Department of Defense, including documents containing sensitive personnel information and even classified data. To take it one step further. CCIU attempted to replicate the process by which individuals can locate and obtain sensitive documents leaked via P2P networks. Using one computer connected to the Limewire P2P network over a five day period, CCIU office was able to identify and download the following documents:

- Three Enlisted Record Briefs
- One Officer Record Brief
- One Noncommissioned Officer Evaluation Report
- One Officer Evaluation Report
- One Leave and Earning Statement

Also found were two completed tax returns, a résumé, a medical record, insurance documents and many other official and personal documents of Soldiers

YOUR “PEERS”:

In February 2009, the Today show covered the danger of accidental data leakage via P2P networks. Their research estimated that “more than 150,000 tax returns, 25,800 student loan applications, and nearly 626,000 credit reports” were then currently exposed via P2P networks. These are only a few examples of sensitive personal and professional documents that can be found on P2P networks, the release of which to the wrong person could be devastating. With relative ease, cyber criminals, identity thieves, scam artists, terrorists, and foreign intelligence officers can pick this low hanging fruit, using low-tech methods, while maintaining near or total anonymity. What’s worse is that once your documents enter the flow of a particular P2P network, they can be hosted by numerous “peers,” downloaded by hundreds and even jump to different P2P networks where the process will begin again. As you might have deduced, controlling the spread and utilization of your data once this happens will be next to impossible.

How to Plug Those Leaks:

If you absolutely must use P2P applications on a computer, follow these rules to keep your personal and professional data safe:

- Never install P2P applications on U.S. Government computers that you are authorized to take home, even if you only connect to P2P when you are at home or travelling.
- Never work with or store documents labeled For Official Use Only (FOUO) or Sensitive But Unclassified (SBU) on any computer that has P2P applications installed.
- Never work with or store documents that contain the Personally Identifiable Information (PII) of service-members, including but not limited to Social Security Numbers, home addresses, dates of birth and places of birth, on any computer that has P2P applications installed.
- Review the settings of your chosen P2P application in detail to ensure you know exactly what you are sharing with the P2P network.
- Control the ability to change the settings of your P2P application by restricting privileges on your computer system to yourself and those whose judgment you trust.
- When possible, install P2P applications on a computer, virtual machine, or separate operating system utilized solely for the purpose of P2P activity.

Peer-to-Peer Security Resources and 2CAN References:

Ipoque Peer-to-Peer Statistics
http://www.ipoque.com/news-and-events/news

Committee on Oversight and Government Reform – U.S. Congresses First and Second Investigation into Data Leakage via Peer-to-Peer
http://oversight.house.gov/story.asp?ID=1424

The Washington Post Online – U.S. Congresses Third Investigation into Data Leakage via Peer-to-Peer – Links to Letters Sent to Peer-to-Peer Industry Leaders
http://voices.washingtonpost.com/securityfix/2009/04/congress_to_probe_p2p_data_bre.html?wprss=securityfix

Today Show Segment on Peer-to-Peer Data Leakage
http://today.msnbc.msn.com/id/26184891/vp/29405819#29405819

The United States Computer Emergency Readiness Team (US-CERT):
http://www.us-cert.gov/cas/tips/ST05-007.html

Get Safe Online – Peer-to-Peer Safety
http://www.getsafeonline.org/nqcontent.cfm?a_id=1137

ICE

CCIU is now using the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to provide us with feedback.

Disclaimer: The appearance of hyperlinks in this 2CAN, along with the views and opinions of authors, products or services contained therein does not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations. Such links are provided consistent with the stated purpose of this 2CAN.

CCIU's "Toucan Lan" keeps an eye on cyber crime issues of interest to the Army community.