



STEALTHWATCH IDENTIFIES ILLEGAL FILE SHARING ACTIVITY AND RESPONSIBLE USERS

File sharing is a technology with many legal and beneficial uses, but is easily subject to copyright infringement when users give away and/or accept copyrighted materials without permission. The Recording Industry Association of America (RIAA) was established to protect the intellectual property rights of musicians and opposes the unauthorized file sharing of its music. Since its inception, RIAA has filed file multimillion dollar lawsuits against offenders, including individuals and institutions. Additionally, the U.S. Digital Millennium Copyright Act (DMCA) went into effect on October 28, 1998, criminalizing users who gain unauthorized access to copyrighted works.

Implications for Institutions of Higher Learning

Legally neither RIAA nor those acting under the DMCA can contact students directly, but must rather contact and work with the universities to process claims and identify offenders. Because students frequently engage in file sharing activity, both RIAA and the DMCA pose new challenges for institutions of higher learning. These institutions must protect the privacy and academic freedom of the students, while minimizing:

- Administrative burden associated with processing RIAA and/or DMCA related claims
- Legal and financial risks, thereby protecting institutional reputation
- Network bandwidth consumed by illegal file sharing

Individually these challenges are easily addressed, but together they pose a difficult balancing act.

"For example, if the institutions' reputation is paramount, a ban on peer-to-peer (P2P) traffic is a possibility. Such a ban automatically addresses workload, bandwidth, and legal risk but also potentially encroaches on privacy and academic freedom." ¹

Consequently, universities must educate students on the proper use of file sharing technologies and network policies in order to:

- Promote good network citizenship
- Reduce the number of repeat offenders
- Identify individuals for which illegal file sharing activity is symptomatic of a bigger problem



What Can Be Done to Address These Challenges?

"It's important to distinguish the real concern: not content monitoring per se (after all, antivirus software does this), but crossing the threshold from the routine, automated inspection of traffic into surveillance, or monitoring of behavior." ¹

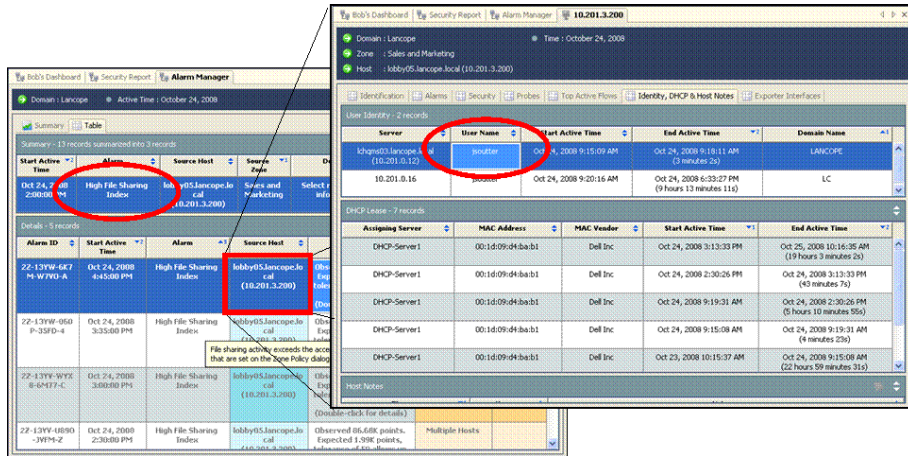
In addition to policies and increased student education and awareness, a non-invasive technology-based deterrent is needed to automatically monitor actual user behavior. The appropriate technology should:

- Conduct IP-to-ID mapping to tie host to end user
- Alarm on high traffic hosts, specifically file sharing hosts, to quickly identify potential abusers of file sharing technology
- Detect anomalous behavior where network activity deviates from the norm
- Log user activity to help track both initial and subsequent infringement activities

How the StealthWatch System and StealthWatch Identity Helps

Lancope's StealthWatch® IDentity appliance gives security and network administrators the ability to automatically determine who is responsible and who is affected when unexpected events happen anywhere on an enterprise network. This powerful, cost-effective solution combines StealthWatch's flow-based Network Behavior Analysis (NBA) and Response technology with advanced user tracking to deliver a direct linkage between individual user logins and specific network events.

Figure 1: StealthWatch drills down from the High File Sharing Index alarm into the user identity tab of the Host Snapshot



About Lancope, Inc.

Lancope®, Inc. is the leader in NetFlow Analysis and the provider of the StealthWatch® for flow-based anomaly detection and network performance monitoring. Delivering unified visibility across physical and virtual networks, StealthWatch eliminates network blind spots and reduces total network and security management costs.

Lancope Headquarters

3650 Brookside Parkway
Suite 400
Alpharetta, GA 30022

+1.770.225.6500 (US)
888.419.1462 (Toll Free)
+1.770.698.8827 (International)

Website: www.lancope.com
E-mail: sales@lancope.com

Requirement	StealthWatch Solution
IP-to-ID mapping	The StealthWatch IDentity product taps into a wide range of identity stores to determine the appropriate user of that IP during the timeframe specified.
Alarming on high traffic users	StealthWatch provides a File Sharing Index, a simple visual cue that provides an at-a-glance indicator of user(s) involved in File Sharing Activity. The StealthWatch System also alarms on high traffic conditions (among other anomalous conditions) and the user(s) responsible.
Detection of anomalous user activity	StealthWatch establishes a baseline of normal host behavior. StealthWatch alarms when the host behavior crosses the threshold indicating abnormal network usage.
Logging of initial and subsequent user copyright infringements	StealthWatch maintains a log of user sign-on activity and historical host behavior. Among the dozens of host specific fields, StealthWatch also provides a searchable host notes field, one way to indicate whether the student's file sharing activity involved copyright infringement.

Educause Identity Management Services Program (IMSP)



A proud supporter of the EDUCAUSE Identity Management Services Program (IMSP), Lancope helps academic institutions protect their networks and enhance network and security operations with preferred member pricing for Lancope's identity tracking solution the StealthWatch IDentity appliance, a component of the award-winning StealthWatch System. For more information, visit <http://www.educause.edu/LancopeProductsandServices/12827>

©2009 Lancope, Inc. All rights reserved. Lancope, StealthWatch, and other trademarks are registered or unregistered trademarks of Lancope, Inc. All other trademarks are properties of their respective owners. StealthWatch is covered by U.S. Patent Nos. 7,290,283; 7,185,368; 7,475,426; 7,512,980 and other U.S. and foreign patents pending.

MB11042009

¹ Educause Quarterly, vol. 31, no. 4 (October-December 2008)