

Illegal and Insecure

Companies fail to protect against P2P

MARCH 2008



Executive Summary

This paper presents a study performed by Isis Forensics which investigated the degree to which large businesses are compromised by Peer-to-Peer (P2P) applications. Using our P2P Observer software we analysed the proportion of FTSE 100 and Fortune 100 businesses using the Bittorrent file sharing network during a three month period. We found that a significant proportion of businesses listed on the FTSE and Fortune indexes are compromised by file sharing applications and furthermore, we found that illegal behaviour is wide-spread amongst these business users.

Key findings:

- *More than **35%** of FTSE 100 companies participated in file sharing. Of these, **more than 87% were engaged in illegal activity** – predominantly the sharing of copyrighted files.*
- *More than **54%** of Fortune 100 companies participated in file sharing. Of these, **more than 96% were engaged in illegal activity**.*
- *The penetration of business networks by file sharing applications is dependent upon business type. In the FTSE 100, hospitality and shipping related industries are the most vulnerable. For the Fortune 100, it is high-tech and manufacturing companies.*

*P2P file sharing software puts businesses at risk of legal action, threatens network security, may significantly increase network costs and can lead to lost productivity. Given these risks, it is **critical** that businesses secure their networks against the threat posed by P2P.*

Monitoring P2P Usage

Peer-to-Peer (P2P) has revolutionised how people use the internet to communicate with one another, empowering users to produce and distribute content free from any form of control or censorship by third parties. Today it is widely accepted that P2P applications (for example, Lime Wire, Bear Share, Bittorrent, etc) are responsible for the vast majority of internet traffic.

This study has been performed using the Isis Forensics P2P Observer system. The P2P Observer system uses state of the art technologies to monitor and analyse P2P network usage. In contrast to many existing monitoring technologies, the P2P Observer System can perform monitoring externally from an organisations network, observing data at the P2P level, in real-time as it is broadcast from business networks. A key advantage of this approach is that Isis Forensics can observe P2P usage on business networks without having to gain access to the network being observed. This makes it impossible for Isis Forensics' monitoring activities to interfere with critical business applications.

This study analysed the Bittorrent P2P file sharing system over a period of three months from June to August 2007. During this period the P2P Observer software logged Bittorrent messages being broadcast from around the world, identifying messages originating from business networks for further analysis. We analysed over 42 thousand active torrents, observed over 12 million distinct users and gathered a total of 4.3GB of data.

Bittorrent is the most popular P2P file sharing system, and is estimated to consume more bandwidth than any other Internet application¹. Bittorrent adopts an enforcement approach to sharing - in order to download files from the network users are also required to re-distribute pieces of this same file. Such an approach benefits file distribution, but it poses a particular problem for business networks, as the redistribution process incurs additional network costs and legal risks.

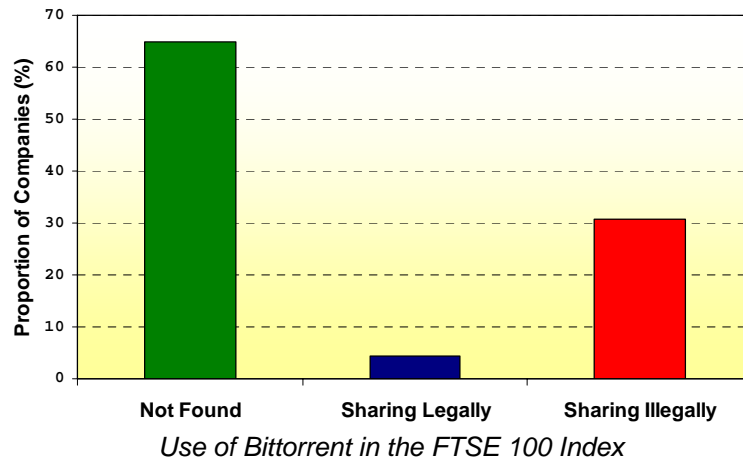
We analysed our trace data for messages originating from each business listed on the FTSE 100 and Fortune 100 indexes. This data was then classified as either legal or illegal (i.e. referencing copyrighted or illegal pornographic material).

¹ *Is P2P Dying or Just Hiding?*, Karagiannis, T., Broido, A., Brownlee, N., Faloutsos, M., December 2004.

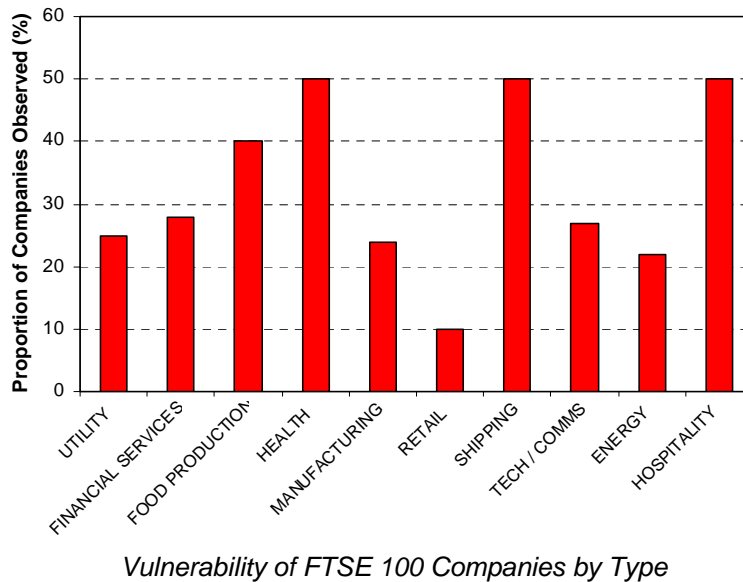
File Sharing in FTSE 100 Companies

We analysed the scale and characteristics of file sharing occurring through the networks of companies listed in the Financial Times Stock Exchange ranking of the top 100 U.K. companies (the FTSE 100).

Analysis showed that a significant proportion of FTSE 100 companies participated in file sharing – over 35%. Of these, the overwhelming majority – more than 87% participated in illegal activity, primarily copyright infringement.



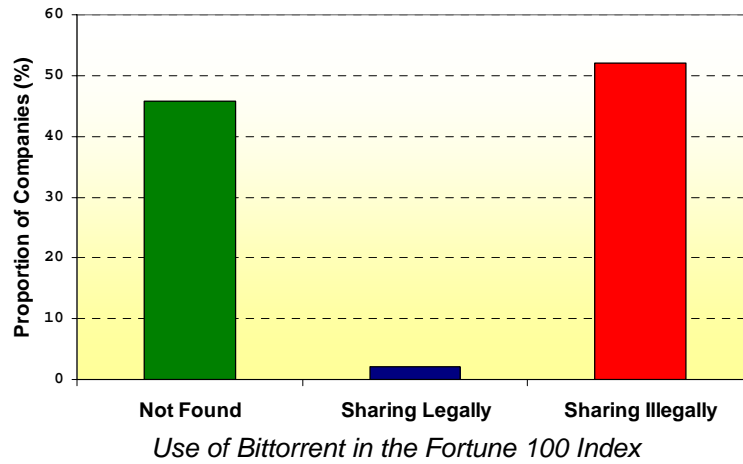
We performed further analysis, classifying FTSE 100 companies by their business type. This revealed that in the FTSE 100 index the most vulnerable industries are health, hospitality and shipping.



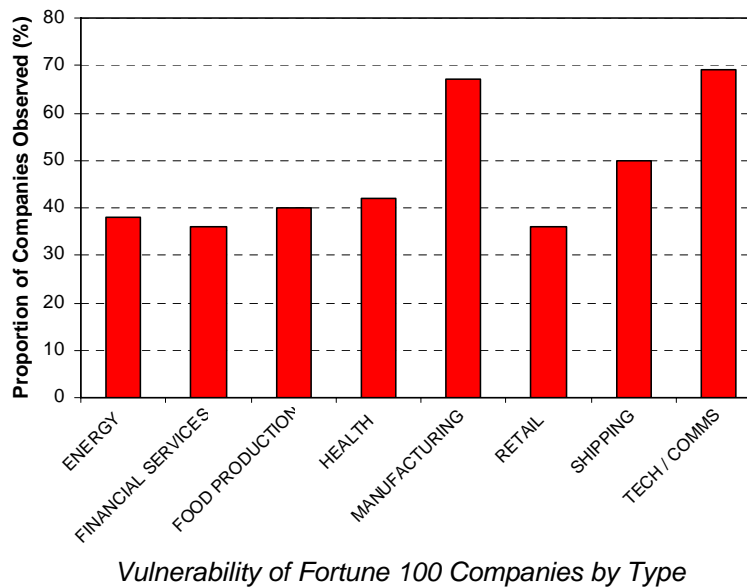
While file sharing poses significant problems for all businesses, for those businesses networks which deal with highly confidential documents it should be of particularly grave concern. Despite this, industries which are highly dependent upon intellectual property such as the manufacturing, technical and communications companies appear to be amongst the most vulnerable, as are businesses which deal with confidential records such as the health industry and, to a lesser extent, the finance industry.

File Sharing in Fortune 100 Companies

Our analysis found that the majority of Fortune 100 companies participated in the Bittorrent file sharing network – over 52%. Of these, illegal behaviour is even more widespread than for participating FTSE 100 companies – with more than 95% participating in illegal activity.



Business classification showed that the most vulnerable businesses are those in the manufacturing, shipping and technical / communications industries.



The Organisational Risks of File Sharing Software

Unfortunately, although P2P file sharing software can be seen to bring benefits to some, from a business perspective it brings significant risks.

Danger of Legal Action

Over 95% of all files available on P2P file sharing systems are copyrighted and in most countries, including the US, Canada, UK and Australia, business can be held responsible for any copyright infringement committed using their network. Each year thousands of copyright lawsuits are filed seeking millions in compensation. However, copyright infringement is not the only illegal activity occurring on P2P file sharing systems. Studies have also shown that hundreds of thousands of searches for illegal pornographic material (including images of child abuse) are performed each day, and several aggressive new initiatives designed to prosecute this activity have recently been launched. In either case, businesses have an ethical and legal obligation to secure their networks against the legal threats posed by P2P file sharing systems.

Security Threats

Viruses and Trojan-horse programs are widespread on P2P file sharing systems, dramatically increasing the risk of your business network being compromised. Furthermore, P2P users have often been observed accidentally sharing sensitive corporate files, including classified information as explored in the recent report by the U.S. Patents and Trademark Office. Where businesses are observed distributing significant volumes of data on P2P file sharing systems, there is also the risk that this may be due to hacked, or 'zombie' machines, which under the control of an external party may be used to participate in various forms of illegal P2P activity.

Increasing Company Costs

Files available on P2P systems tend to be significantly larger than those available on the web, and file popularity is highly concentrated and dynamic. This means that P2P applications generate large and unpredictable network loads that have the potential to swamp network links, interfere with an organisations critical Internet services and, crucially, significantly increase the cost of provisioning and administering your network. Extensive anecdotal evidence has also shown that P2P systems can significantly, yet invisibly increase business networking costs, in some cases forcing companies to implement expensive upgrades simply to support the (unseen) file-sharing activities of their employees.

Damage to Company Reputation

While P2P users may think themselves anonymous, in reality they are far from it. Any time that a user participates in P2P file sharing, they broadcast their details and the details of their access provider across the Internet. Given the unsavoury nature of much P2P content, this exposes companies which support P2P use to considerable potential embarrassment.

Lost Productivity

Our experiments have shown that employees spend a significant amount of time using P2P file sharing systems during business hours (often as much as an hour a day), thus leading to an inevitable loss in productivity.

Given the serious legal, financial, security and productivity problems that P2P applications cause for business networks, it is particularly critical that leading companies, such as those listed in the Fortune and FTSE 100 indexes take steps to restrict their use.

Summary

This study has analysed the extent and characteristics of Bittorrent file sharing usage by companies listed on the FTSE 100 and Fortune 100 indexes.

Our analysis has shown that a significant proportion of FTSE 100 and Fortune 100 companies have file sharing software running on their networks and that this software is being used to support wide-spread illegal activity within these organisations.

Analysing the compromised FTSE 100 and Fortune 100 companies by industry, we find that the health, hospitality, shipping, manufacturing, high-tech and communications industries are particularly vulnerable to being compromised by P2P file sharing software.

P2P file sharing software puts businesses at risk of legal action, threatens network security, may significantly increase network costs and can lead to lost productivity. Given these risks, it is critical that businesses secure their networks against the threat posed by P2P. Isis Forensics offers a suite of services tailored to securing business networks against the threat posed by P2P and giving businesses back control of their networks.

Isis Forensics is an international security consultancy firm which specialises in securing business networks against Peer-to-Peer (P2P) and file sharing technologies. Isis Forensics professional solutions are designed to minimise the legal, security and financial risks that file sharing poses to business networks.

For more information about how we can help you, contact us at:

Isis Forensics

PO Box 793

Lancaster

Lancashire

LA1 9ED

UK

Tel:+44(0)7092 891873

Fax:+44(0)7092 891895

Email:enquiries@isis-forensics.com

Web: www.isis-forensics.com