

FILE SHARING



Legal music and video sites may attract serious traffic, but they're dwarfed by the top three BitTorrent sites, which attract more than a billion visits a month.

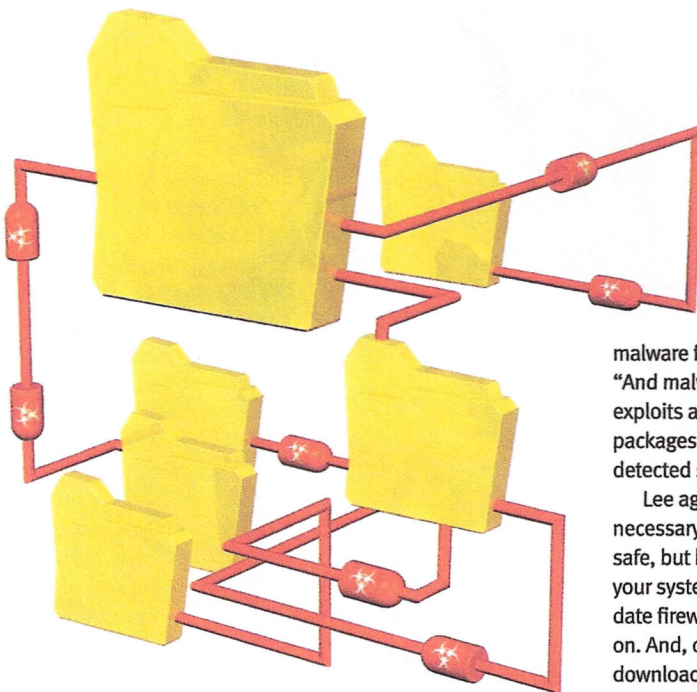
Numbers like that mean BitTorrent presents a huge opportunity for criminals. There's no need to set up fake websites or hack into existing ones: attackers can simply seed an infected file with an attractive-sounding name and let human nature do the rest.

"It comes down to people's desire for games, cracks, pornography and so forth," says Andrew Lee. "People just want to download Photoshop or whatever. They're not thinking about risks. If you see a file called 'Britney Spears naked'... well, perhaps that's not so attractive any more... but there was a time when a lot of people would have downloaded that and got infected."

What's more, once a poisoned download has been seeded into the BitTorrent community, the attacker can disconnect and disappear. Due to the way peer-to-peer file sharing works, the poisoned file will remain available for as long as there's a single, unwitting victim hosting it.

To take a representative sample of the risk, we downloaded every executable package that had been uploaded to one of the major BitTorrent websites on a given day, plus a selection of popular games and applications (having disabled the client's upload facility, so that we wouldn't ourselves be distributing copyright material).

Out of 79 torrent files, we found nine



contained malware. One was an old torrent of Unreal Tournament; the other eight purported to be recent releases of tools such as DivX Pro and Snagit and games, including ShoppingBlocks and Brain Challenge. In most cases, the installation file was in reality a trojan, which should be picked up by antivirus software, but on a couple of occasions the software came with an extra file, such as a serial number generator, which would try to install malware.

That 11% infection rate is certainly worrying, but things could have been much worse. BitTorrent's constituency tends to be more aware of the risks than a casual user, and when they find a malicious download they're likely to delete it straight away, rather than continuing sharing. What's more, most torrent sites detail the number of people sharing each file: if this number is surprisingly small, that's a clue that it may not be what it seems. On many sites, visitors can leave comments about the files they've downloaded: on checking the comments, we found the infected Unreal Tournament torrent had been accompanied by a warning to steer clear.

"BitTorrent users have recognised the danger, and in response some of them have become more cautious and more collaborative," says Bridwell.

All the same, community moderation can't make BitTorrent entirely safe. The three infected

applications we downloaded had only recently been made available, and no-one had yet flagged them up as bogus. "The problem is that, with downloads such as this, someone has to find the

malware first," Bridwell explains.

"And malware writers test out their exploits against the common antivirus packages to make sure they won't be detected straight away."

Lee agrees that a degree of caution is necessary. "I think that BitTorrent can be safe, but be sensible," he warns. "Keep your system patched, and keep an up-to-date firewall, antivirus package and so on. And, obviously, I don't advocate downloading anything illegitimate."

» LimeWire

There are several other widely used file-sharing systems including LimeWire, Shareaza and eMule. These work on a similar principle to BitTorrent, but there's no central website showing information about a given download. Thus, there's no way to warn others if a file is infected, and you can't necessarily see how many peers are sharing a given file.

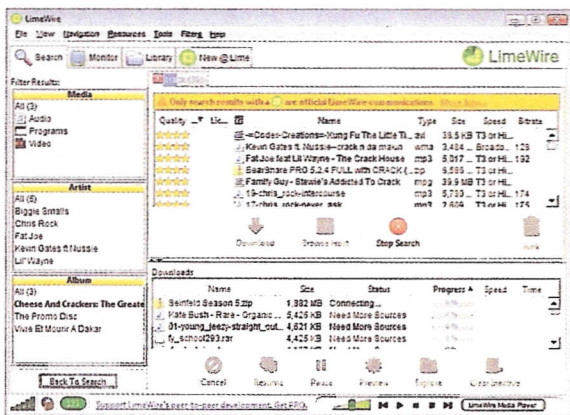
We anticipated these systems might be less safe than BitTorrent, but were shocked at how right we were. We used LimeWire to download 123 randomly selected files. A remarkable 37 of them contained malware, including the Puper.G and DNSChanger trojans and the Sality virus. Around a third of our infected downloads were deceptively named, with executables made to look like music files.

A 30% infection rate is worrying enough, but it isn't the only risk associated with LimeWire and its companions. These clients share entire folders, rather than individual files as with BitTorrent, making it possible to accidentally share more data than intended. This could result in your personal data being lost, or even legal consequences if you end up sharing copyrighted material.

Yet these programs remain popular, especially among teens. "There are masses of teenagers using things like LimeWire," observes Kaspersky's David Emm. "David Phillips, who runs a malware course at the Open University, gives talks to teenagers about malware. And when he describes the particular risks of file sharing, you can see from the sheepish looks that they've all encountered these problems."

RISK RATING HIGH

If you're downloading pirated material, expect to be attacked repeatedly. Your safest course of action is to steer clear of the entire scene.



Clients like LimeWire could lead to you sharing more data than you want.

