

Searching for Malware in BitTorrent

Andrew Berns

22C:169 Computer Security Presentation

April 29, 2008

adberns@cs.uiowa.edu

Topics to Cover

- **Who** cares?
- **How** was malware found?
- **What** was discovered?
- **Where** can these statistics be used?
- **When** will this information be inaccurate?

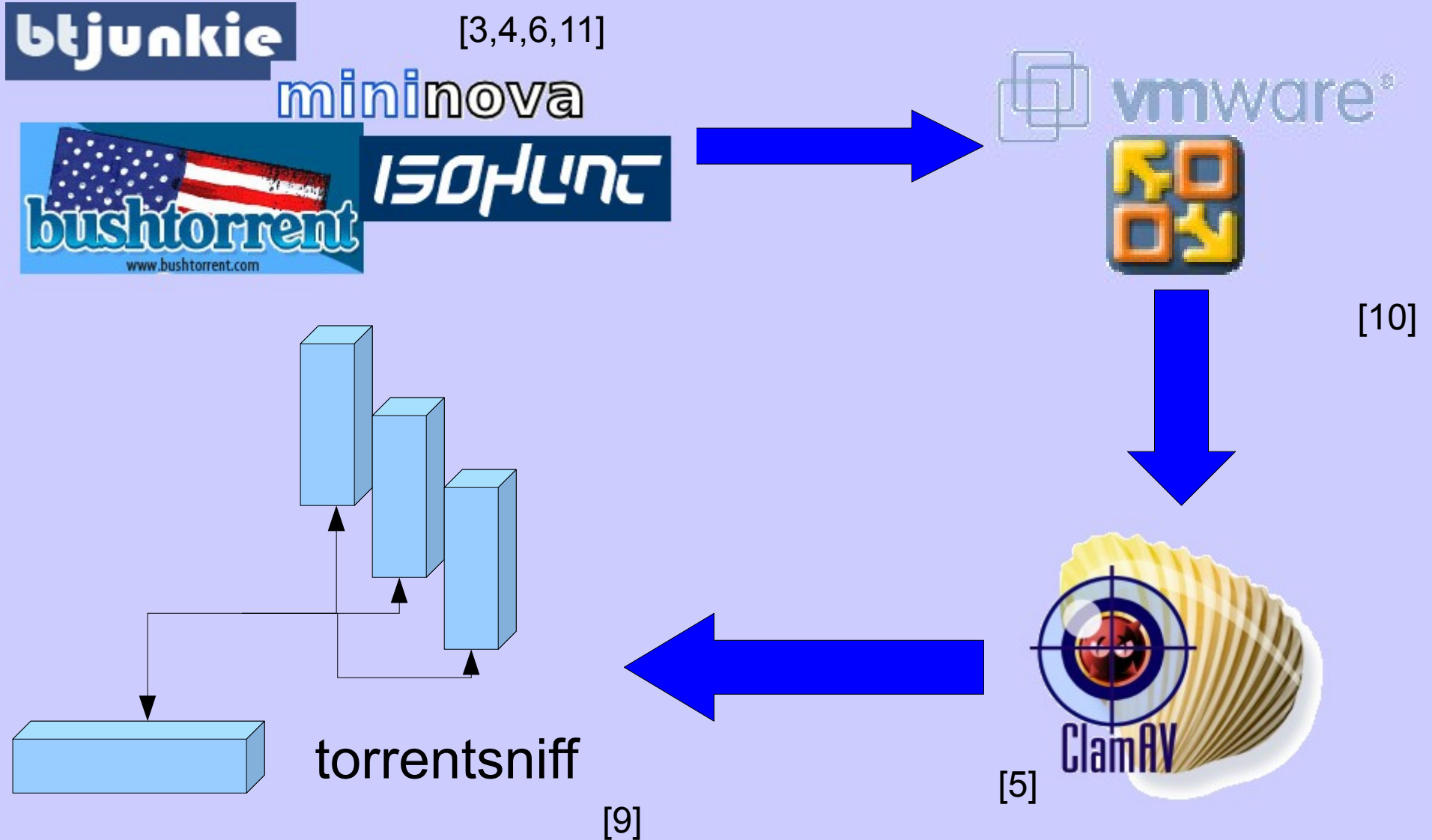
Who Cares?

? ! ?

Who Cares?

- P2P traffic has been estimated as using up around 70% of Internet bandwidth [2]
- BitTorrent is the second most popular P2P system (eDonkey is the first) [2]

How?



What was found?

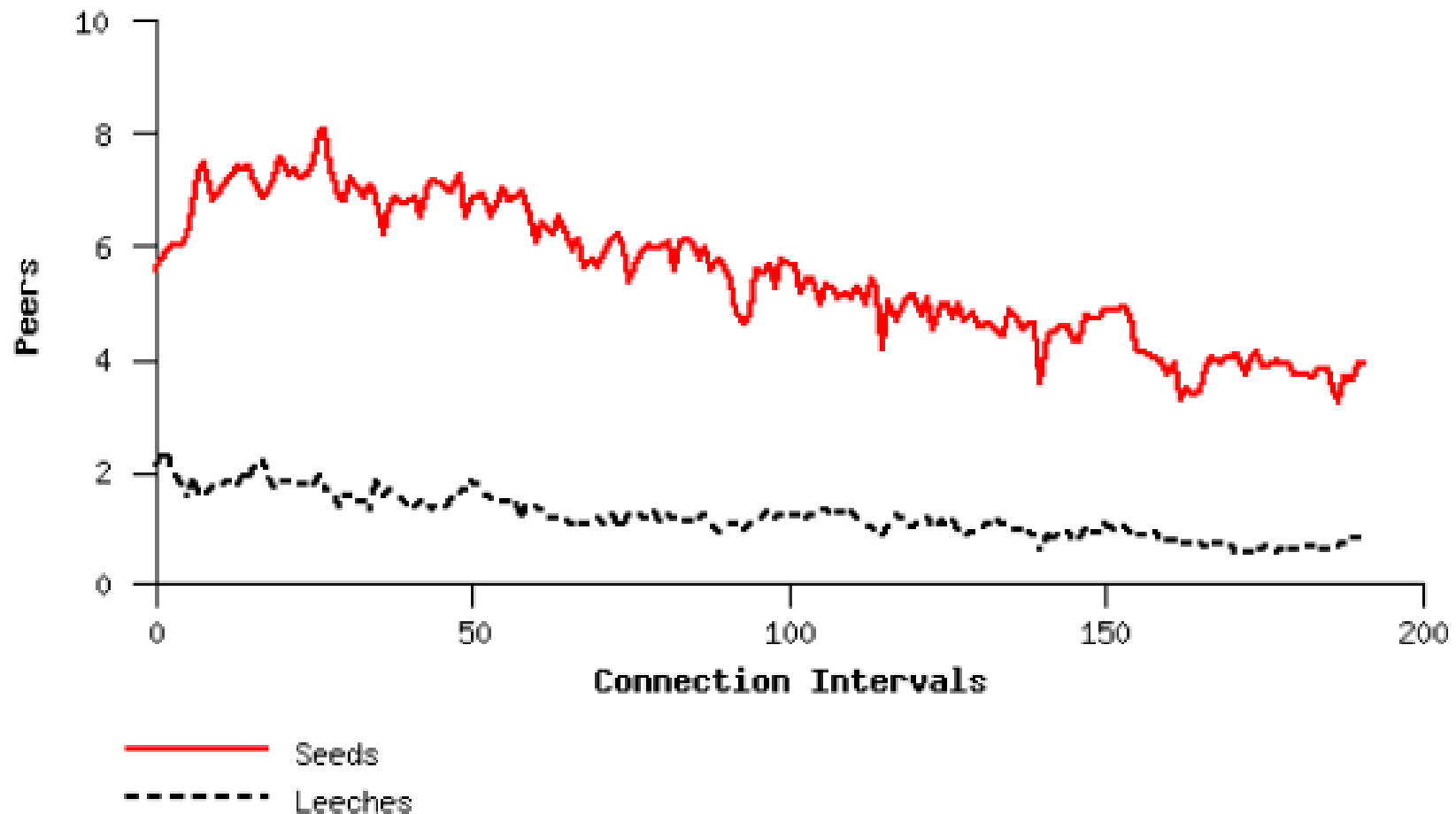
- Malware was quite common in the sample
 - 70 out of 379 downloads had malware (18.5%)
- The majority of malware appeared more than once
 - Trojan.Small-5335 (22 times), Trojan.Zlob-3743 (8 times)
- Fifteen infected files were for keygens / activation tools, six were for other P2P file-sharing applications

Findings, cont.

- Malware had a lower average connection time than the fourteen clean files
 - 5 hours, 25 minutes (malware)
 - 9 hours, 25 minutes (clean)
- Over 90% of infected torrents were connected less than 12 hours, 30 minutes
 - 22 hours, 30 minutes for 90% of clean files

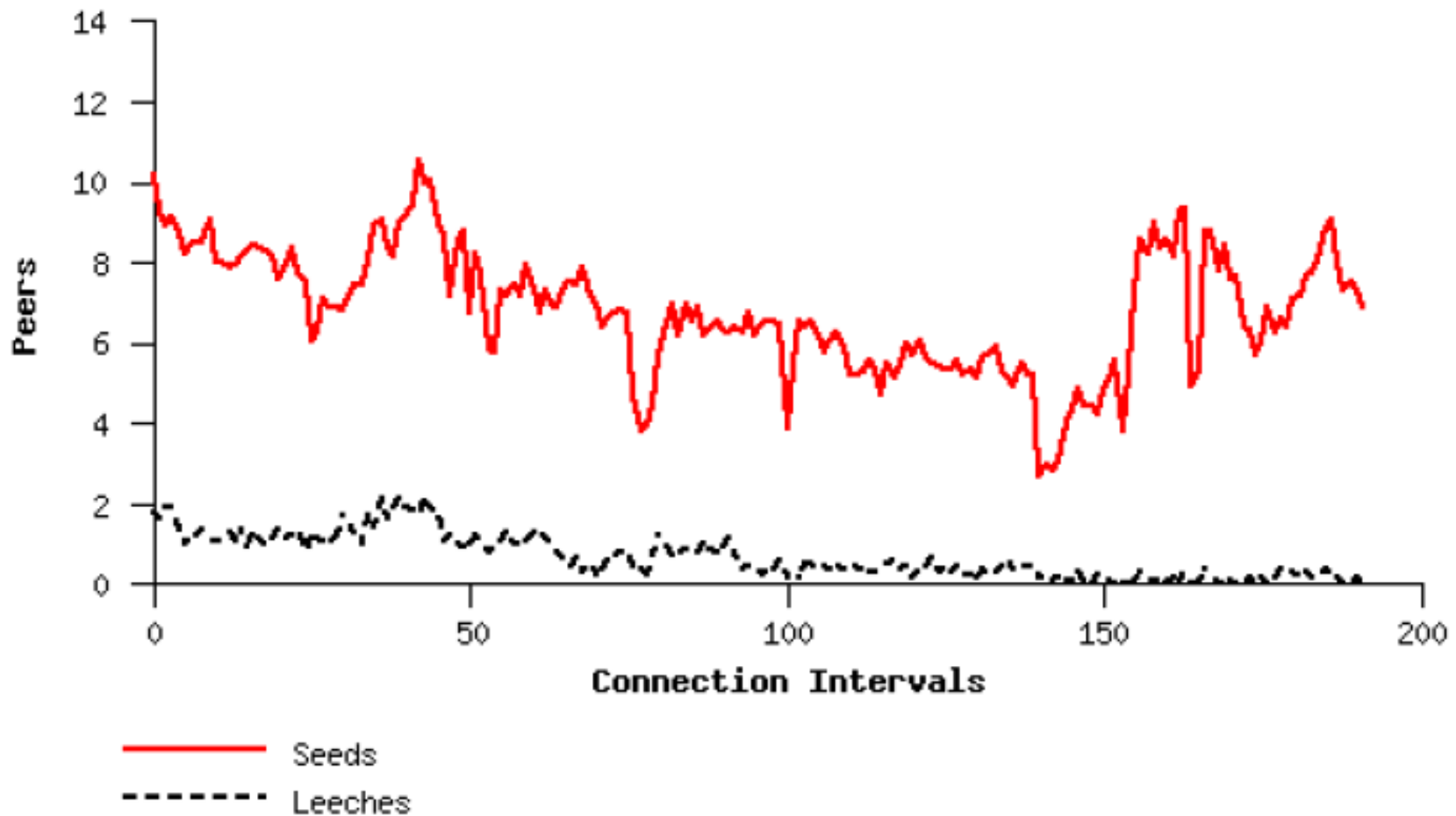
Findings, cont.

Figure 1: First Four Days of an Infected Torrent

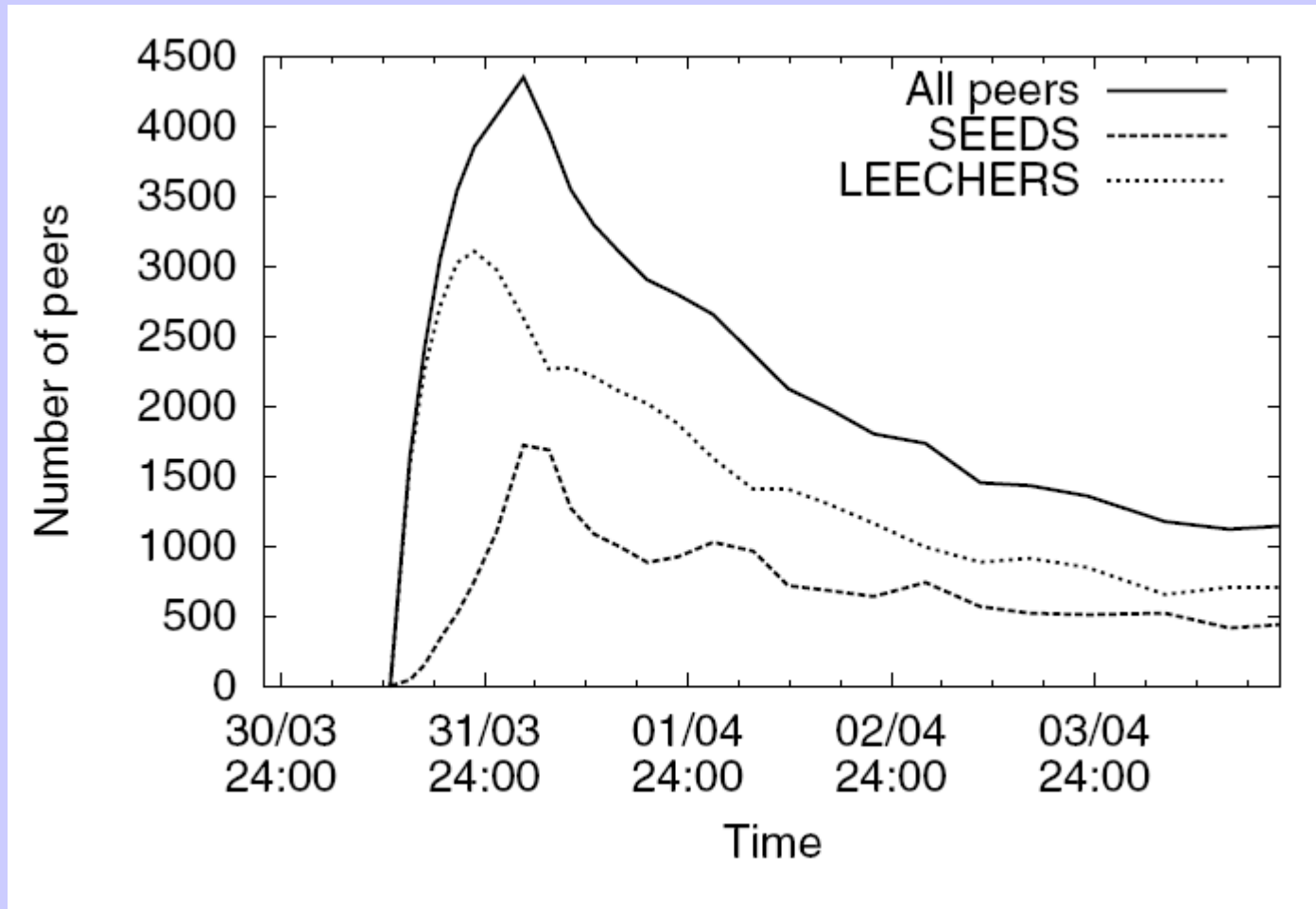


Findings, cont.

Figure 2: First Four Days of a Clean Torrent



Findings, cont.



Where is this useful?

- Simple filtering rules – for example,
 - Do not download torrents with low seed counts
 - If torrent did not have initial flash crowd, be suspicious
 - If more seeds than leeches, use caution
- User awareness for avoidance
 - Steer clear of unpopular key generation utilities
 - Be wary of “new” versions with low seed counts

When is it wrong?

- Seed and leech counts seem easy to fake
 - Accidentally did so at start of the project
- Case 1: Attacker controls tracker
 - Changed one line of code in the mainline BitTorrent tracker program (`bttrack [1]`) to make torrent appear to have 5000 seeds

When is it wrong?

- Case 2: Attacker does not control tracker
 - Using a few lines of additional code to torrensniff, inflated the seed count of a test torrent to over 300 in less than a minute
 - Can inflate as fast as HTTP requests can be sent

Final Thoughts

- Malware is spread with the BitTorrent protocol – but not as much as with other P2P systems! [8,11]
- Simple filtering rules are not sufficient – but what about more advanced rules?
- BitTorrent has several “centralized” points, which may help weed out bad torrents

Questions?

Thank you!

References

- [1] BitTorrent. At <https://launchpad.net/ubuntu/+source/bittorrent/>
- [2] “BitTorrent: the 'one third of all internet traffic' myth” Accessed April 1, 2008 at <http://torrentfreak.com/bittorrent-the-one-third-of-all-internet-traffic-myth/>
- [3] BTJunkie. At <http://btjunkie.org/>
- [4] BushTorrent.com. At <http://www.bushtorrent.com/>
- [5] ClamAV. At <http://www.clamav.net/>
- [6] isoHunt. At <http://isohunt.com/>
- [7] M. Izal, G. Urvoy-Keller, E.W. Biersack, P.A. Felber, A. Al Hamra, and L. Garces-Erice. Dissecting BitTorrent: five months in a torrent's lifetime. In *Passive and Active Network Measurement*, 2004
- [8] A. Kalafut, A. Acharya, and M. Gupta. A study of malware in peer-to-peer networks. In *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, 2006
- [9] Torrentsniff. At <http://www.highprogrammer.com/alan/perl/torrentsniff.html>
- [10] VMWare Server. At <http://www.vmware.com/products/server/>
- [11] K. Zetter. “Kazaa delivers more than tunes.” *Wired News*, January 9, 2004. Accessed April 8, 2008 at <http://www.wired.com/techbiz/media/news/2004/01/61852>