



Botnets, Pirates, and Cybercriminals

What are the current trends??

Mark Ishikawa
March 31, 2009
Los Angeles, CA

ALSTON+BIRD_{LLP}



Scope of Online Intellectual Property Piracy

- Estimated 60 million people using file sharing applications worldwide at any given time
- Available content includes movies, TV shows, music, software, video games, audio books
- BayTSP finds 16 million to 18 million infringements of client intellectual property online daily and sends more than 1 million takedown notices monthly.

ALSTON+BIRD_{LLP}

Downloading as easy as using Google

Search Torrents | [Browse Torrents](#) | [Recent Torrents](#) | [TV shows](#) | [Music](#) | [Top 100](#)

All Audio Video Applications Games Other (search titles only)

Browse Torrents

Audio
[Music](#), [Audio books](#), [Sound clips](#), [FLAC](#), [Other](#)

Games
[PC](#), [Mac](#), [PS2](#), [XBOX360](#), [Wii](#), [Handheld](#), [Other](#)

Video
[Movies](#), [Movies DVDR](#), [Music videos](#), [Movie clips](#), [TV shows](#), [Handheld](#), [Highres - Movies](#), [Highres - TV shows](#), [Other](#)

Applications
[Windows](#), [Mac](#), [UNIX](#), [Handheld](#), [Other OS](#)

ALSTON+BIRD LLP

Business Software often infected with malware and spyware

Type	Name	Uploaded	Size	SE	LE
Applications > Windows	WinRAR_3.80_Professional	11-13 2008	1.25 MiB	2058	16
Applications > Windows	Adobe Photoshop CS4 Extended [clean][blaze69] 7z	02-20 18:10	891.35 MiB	2030	498
Applications > Windows	Adobe CS4 Master Collection(Purchased from Adobe.com)-Shadeyman	12-19 2008	5.43 GiB	1727	3508
Applications > Windows	Microsoft Office 2007 Enterprise Edition [blaze69]	02-20 07:25	558.85 MiB	1649	229
Applications > Windows	Windows 7 build 7057 x86	03-12 01:44	2.51 GiB	1526	1574
Applications > Windows	Adobe Photoshop CS3 Extended + Crack	01-08 2008	568.4 MiB	1341	163
Applications > Windows	Nero 7.10.1.0	07-28 2007	173.64 MiB	1336	51
Applications > Windows	Nero 9.0.9.4b (ahead nero) Full install + patch	03-20 14:42	592.06 MiB	1306	537
Applications > Windows	AVG Antivirus 8 0 + serial (EXPIRES YEAR 2018) (CLEAN) [blaze69]	02-20 04:28	59.46 MiB	1219	81
Applications > Windows	WINDOWS XP SP3 2009 ULTRA EDITION	12-30 2008	688.89 MiB	1143	286

ALSTON+BIRD LLP

Popular Music Packaged With Malware



..7	Quality	Lice...	Name	Type	Size	...	Bitrate
13	★★★★★		u2 - with or without you	mp3	4,626	...	128
12	★★★★★		U2 - Get On Your Boots (New Single 2009)	mp3	7,977	...	320
9	★★★★★		U2 - Get On Your Boots	mp3	3,193	...	128
7	★★★★★		U2 - City of Blinding Lights	mp3	5,440	...	128
6	★★★★★		U2 - Beautiful Day	mp3	5,723	...	192
5	★★★★★		U2 - Get On Your Boots (New Single 2009)	mp3	7,981	...	320
4	★★★★★		U2 - Vertigo	mp3	5,923	...	253
4	★★★★★		U2 - I Still Haven't Found What I'm Looking For	mp3	4,351	...	128
4	★★★★★		U2 - Sunday Bloody Sunday	mp3	4,362	...	128
3	★★★★★		u2	mov	3,340	...	
3	★★★★★		06 Get On Your Boots	m4a	6,948	...	T1 256
3	★★★★★		u2	zip	543.6	...	
3	★★★★★		U2 - Angel Of Harlem	mp3	3,584	...	128

ALSTON+BIRD LLP

Quick Response Needed to Contain IP leaks

Emergency RADAR - BayTSP's quick response team

- Monitors all major Internet protocols
- Identifies and tracks client assets and immediately notifies client once the leak has been validated.
- Options for high priority scanning, detection logs, takedown notices, reporting and detailed evidence collection for possible litigation.

ALSTON+BIRD LLP

Case Study - Intellectual Property Leak

- Major software company
- Code for highly anticipated software application leaked to the Internet
- Within hours more than 60,000 people were downloading
- Reduced to 600 within one week

ALSTON+BIRD_{LLP}

Thank you!

Mark Ishikawa
BayTSP, Inc.
P.O. Box 1314
Los Gatos, CA 95031
408.341.2300 - phone
408.341.2399 - fax

marki@baytsp.com

<http://www.baytsp.com>

ALSTON+BIRD_{LLP}



Information Security Policy

Threats Response Enforcement

Michael Zweiback
Los Angeles Office

March 31, 2009
Los Angeles, CA

ALSTON+BIRD_{LLP}



Threats In The “Wild”

- State Sponsored - Russian Business Network
- Highly Sophisticated Organized Profiteers
 - Botnet operators and Malware writers who share work through chat channels;
 - Extortion via hacking-Express Scripts Investigation - Threat to publish hacked HIPAA (including SSNs) information detailed in PC World.
- Disgruntled Employees - Vendors/Contract IT
- Hacktivists - Bragging Rights - University Hacking - USC

ALSTON+BIRD_{LLP}

- BotNETs are the growing underworld infrastructure for web disruption and criminal activity.
 - Distributed Denial of Service (DDOS)- Generally for purposes of extortion.
 - Spreading Infection/malware
 - E-Mail SPAM- Most spam is distributed by BotNET



ALSTON+BIRD LLP



ALSTON+BIRD LLP

Development Of An Information Security Plan

- Do you know what you have and why you keep it?
- Have you segregated access so that only those who need sensitive information have access? Where are your Trade Secrets?
- Have you clearly designated responsibilities in the event of a security breach?
- If the effected technology platform is outsourced how do you obtain access? What are your access rights?

ALSTON+BIRD_{LLP}

How Do You Respond?

- So you get the 3:00 a.m. call- Are you ready to act?
- Do you have a response plan? Who do you need?
- Start small and build out;
- IT Staff are your first responders;
- Chief Information Privacy Officer – Coordination;
- HR- if the breach is internal what are the existing privacy policies that impact your ability to obtain information;

ALSTON+BIRD_{LLP}

- **General Counsel's Role- Quarterback**
 - To communicate with C-level executives
 - Insure resources properly allocated and available
 - Coordinate press response, if necessary
- **Outside Counsel Role**
 - Breach notification requirements
 - Timing - Safe harbors for law enforcement
 - If multiple jurisdictions impacted you need to know the laws of each state as well as international jurisdictions.
 - Are you going to need to self-report the incident to regulators?

ALSTON+BIRD_{LLP}

The Regulators

Federal Trade Commission Enforcement under Section 5 of the FTC

- Prohibits unfair or deceptive promises in privacy statements including promises about the security of consumers personal information.
 - FTC v. GUIDANCE SOFTWARE
- Unfairness authority to challenge information practices that cause substantial consumer injury
 - FTC v. TJ MAXX

ALSTON+BIRD_{LLP}

- Penalties for a violation can include:
 - Establish comprehensive security program;
 - Audit every two years by a third party;
 - Reporting to the FTC;
 - If breach demonstrates compliance is seriously lacking, outside monitor may be required;
 - Under regulatory scrutiny for 10-20 years - similar to an injunction.

ALSTON+BIRD_{LLP}

Others Are Also Watching-

- SEC now enforcing “Safeguards Rule” of federal securities laws for broker-dealers and SEC registered investment advisors.
- SEC v. LPL Financial- Sept.11, 2008 -Failure to adopt policies to safeguard customer information – 10,000 customers vulnerable after hacking of online trading platform.

ALSTON+BIRD_{LLP}

Others Are Also Watching-

- SEC Penalties-
 - Cease and desist from future violations of Safeguards Rule;
 - \$275,000 fine;
 - Must retain independent expert to review policies and procedures;
 - Implement a policy and set procedures for training employees to safeguard customer data.

ALSTON+BIRD_{LLP}

You Are Not Done

- FTC-COPA-Sony BMG - Largest FTC Settlement Ever
- Health and Human Services-
 - Providence Health Services - Stolen medical records as a result of lost lap tops; Paid \$100,000 Fine to DOJ
- State Attorneys General -Texas and California very active-enforcement of federal regulatory schemes;
- Increasing Class Action Litigation- Erosion of Actual Damages requirement

ALSTON+BIRD_{LLP}