One Bad Apple Spoils the Bunch

Stevens Le Blond Pere Manils Abdelberi Chaabane
Dali Kaafar Claude Castelluccia Arnaud Legout Walid Dabbous
IP address?
“I am not going to be around this year… sorry for missing out on the beer…”
Background
Roadmap

1) 2 attacks against Tor

2) BitTorrent usage on Tor
BitTorrent on Tor

- Get lists of peers (Tracker, DHT)
- Content distribution
1) Hijacking Tracker Responses

Traced 10,000 IPs
2) The Bad Apple Attack

For each BitTorrent stream, traced 2 additional streams (9% of all streams)
Roadmap

1) 2 attacks against Tor
2) BitTorrent usage on Tor
Over-representation per Country

<table>
<thead>
<tr>
<th>Rank</th>
<th>#</th>
<th>%</th>
<th>Over</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>958</td>
<td>14</td>
<td>0.9</td>
<td>US</td>
</tr>
<tr>
<td>2</td>
<td>937</td>
<td>13</td>
<td>5.6</td>
<td>Japan</td>
</tr>
<tr>
<td>3</td>
<td>887</td>
<td>13</td>
<td>2.8</td>
<td>Germany</td>
</tr>
<tr>
<td>4</td>
<td>369</td>
<td>5</td>
<td>1.3</td>
<td>France</td>
</tr>
<tr>
<td>5</td>
<td>354</td>
<td>5</td>
<td>1.8</td>
<td>Poland</td>
</tr>
<tr>
<td>6</td>
<td>236</td>
<td>3</td>
<td>0.9</td>
<td>Italy</td>
</tr>
<tr>
<td>7</td>
<td>232</td>
<td>3</td>
<td>0.6</td>
<td>UK</td>
</tr>
<tr>
<td>8</td>
<td>231</td>
<td>3</td>
<td></td>
<td>China</td>
</tr>
</tbody>
</table>

Why some countries are over-represented?
BitTorrent Usage in the US

- Porn
- Windows
- Anime
- Highres
- Action
- Retro-Classic
- Applications
- Drama
- Comedy
- Pictures
- Hentai
- Soundtracks
- Documentary
- Crime
- American
- Sci-Fi
- Radio
- Alternative
- Adventure
- Alternative
BitTorrent Usage in Japan

Hentai
BitTorrent Usage in Germany

Over-representations likely due to sociological reasons
Take Home Messages

1) P2P filesharing apps kill privacy on Tor

2) Bad Apple attack can be severe

3) Significant fraction of Tor traffic can be traced with app-level attacks

Stevens.Le_Blond@inria.fr