The Impact of Incentives on Notice and Take-down

Tyler Moore and Richard Clayton

University of Cambridge
Computer Laboratory

7th Workshop on the Economics of Information Security (WEIS)
Dartmouth College
Hanover, NH, USA
June 27, 2008
Outline

1. Introduction
   - Notice and take-down overview
   - Defamation
   - Copyright violations

2. Fraudulent websites
   - Phishing
   - Fake escrow agents
   - Mule-recruitment websites
   - Online pharmacies

3. Child sexual abuse images

4. Comparing take-down effectiveness
Outline

1. Introduction
   - Notice and take-down overview
   - Defamation
   - Copyright violations

2. Fraudulent websites
   - Phishing
   - Fake escrow agents
   - Mule-recruitment websites
   - Online pharmacies

3. Child sexual abuse images

4. Comparing take-down effectiveness
Undesirable content pervades the Internet
Schemes for its removal are called notice and take-down (NTD) regimes
Those who want the content removed get into contact with the responsible ISPs, webmasters
Types of content subject to NTD

- Defamation
- Copyright violations
- Phishing
- Fake escrow agents
- Mule-recruitment websites
- Online pharmacies
- Spam, malware and virus hosts
- Child sexual abuse images
Comparing NTD regimes

- Factors for comparing NTD regimes
  - Incentives for removal on requesting party
  - Formalization of NTD mechanism
  - Legal framework available
  - Hosting strategy used by offenders
  - Speed at which material is removed

- We compare the speed of removal for different regimes, and see how the results match up to the available incentives, legal frameworks and hosting strategies
Defamation

- Laws against defamation are long established
- But defamation has taken on new importance in the Internet context because the bar for publication has lowered plus dissemination has widened
- Legal decisions (UK: Godfrey v. Demon Internet) established that serving notice to ISPs hosting defamatory content should trigger content removal
Copyright violations

- DMCA introduces legal principle of ‘safe harbor’ to ISPs compliant with take-down requests from rights holders
- DMCA also requires ISPs receiving ‘put-back’ requests to return the content if the owner agrees to stand behind their claim in court
- Patchy data suggests that ISPs remove content to avoid liability without necessarily establishing accuracy of complaints
Outline

1. Introduction
   - Notice and take-down overview
   - Defamation
   - Copyright violations

2. Fraudulent websites
   - Phishing
   - Fake escrow agents
   - Mule-recruitment websites
   - Online pharmacies

3. Child sexual abuse images

4. Comparing take-down effectiveness
Phishing websites impersonate banks to commit identity theft

- Banks issue take-down notices despite no legislative basis
- Hosting options for phishing websites
  1. Compromised machine
     (http://www.example.com/~user/images/www.bankname.com/)
  2. Free webspace
     (http://www.bankname.freespacesitename.com/signin/)
  3. Registered domain (bankname-variant.com) which then points to free webspace or compromised machine
Rock-phish attacks

- Purchase many innocuous-sounding domains (e.g., lof80.info)
- Send out phishing email with URL http://www.volksbank.de.netw.oid3614061.lof80.info/vr
- Gang-hosted DNS server resolves domain to IP address of one of several compromised machines, which proxy to the mothership hosting 20 fake websites

Fast-flux attacks

- Same strategy as rock-phish, except domains resolve to 5 IP addresses for a short time, then abandon them for 5 more
- Forces take-down of domains, not compromised machines
<table>
<thead>
<tr>
<th></th>
<th>Sites</th>
<th>Lifetime (hours)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>mean</td>
<td>median</td>
</tr>
<tr>
<td><strong>Free web-hosting</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>all</td>
<td>395</td>
<td>47.6</td>
<td>0</td>
</tr>
<tr>
<td>brand owner aware</td>
<td>240</td>
<td><strong>4.3</strong></td>
<td>0</td>
</tr>
<tr>
<td>brand owner missed</td>
<td>155</td>
<td>114.7</td>
<td>29</td>
</tr>
<tr>
<td><strong>Compromised machines</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>all</td>
<td>193</td>
<td>49.2</td>
<td>0</td>
</tr>
<tr>
<td>brand owner aware</td>
<td>105</td>
<td><strong>3.5</strong></td>
<td>0</td>
</tr>
<tr>
<td>brand owner missed</td>
<td>155</td>
<td>103.8</td>
<td>10</td>
</tr>
<tr>
<td><strong>Rock-phish domains</strong></td>
<td>821</td>
<td>70.3</td>
<td>33</td>
</tr>
<tr>
<td><strong>Fast-flux domains</strong></td>
<td>314</td>
<td>96.1</td>
<td>25.5</td>
</tr>
</tbody>
</table>
Fake escrow agents

Protect yourself with our Exchange Collect Services!

Welcome

KLM Cargo
Thanks to our innovative view of courier transport and to our commitment to provide a competitive service, we soon were ahead in the sector, leaving all the traditional European companies behind. Since that day, we have continued to work in the same way that allowed us to become leaders: innovation and continuous improvement of our offer.

Services

When should I use Exchange Collect?
Quite simply, you should use Exchange Collect Services whenever

Special Offer
A new service introduced by KLM Cargo helps the money catch up. Exchange Collect Services helps exporters and importers accelerate payments
Fake escrow agents (ctd.)

Welcome to Globe Diplomatic Courier Service.
Thanks to our innovative view of courier transport and to our commitment to provide a competitive service, we soon were ahead in the sector, leaving all the ...
gdcag.com/about_us.htm - 12k - Cached - Similar pages

Welcome to Website
Thanks to our innovative view of courier transport and to our commitment to provide a competitive service, we soon were ahead in the sector, leaving all the ...
www.gsp-express.ro/about_us.htm - 22k - Cached - Similar pages

Welcome to Website
Thanks to our innovative view of courier transport and to our commitment to provide a competitive service, we soon were ahead in the sector, leaving all the ...
www.secure-spedition.ro/ - 25k - Cached - Similar pages

WHO WE ARE?
... AND TO OUR COMMITMENT TO PROVIDE A COMPETITIVE SERVICE, WE SOON WERE AHEAD IN THE SECTOR, LEAVING ALL THE TRADITIONAL EUROPEAN COMPANIES BEHIND. ...
royal-international-shipping.org/who.php - 16k - Cached - Similar pages

Global Shipping Company
Thanks to our innovative view of courier transport and to our commitment to provide a competitive service, we soon were ahead in the sector, leaving all the ...
www.global-delivery-express.com/ - 19k - Cached - Similar pages
Fake escrow agents

- Unlike phishing, fake escrow agents do not impersonate a real business.
- Instead, they impersonate a service.
- Fake escrow agent lifetimes:
  - For 696 fake escrow sites, mean lifetime is 222 hours (24.5 hour median).
  - Bank customers are harmed, but no bank is impersonated so the banks don’t get involved.
  - Only motivated ‘vigilantes’ remove the sites.
  - Longer lifetime than phishing, but surprisingly short.
Mule-recruitment websites
Mule-recruitment websites

1. Regional Sales Manager

Status: Part-time

Job description:
- Work as a member of a group, helping to enlarge a base of customers in countries all over the world and liaise with head office on a daily basis;
- Deliver high standards of customer service ensuring high delivery speed and quality of orders;
- **Manage a part of a sales cycle – ensure fast remittance of payments through your bank account and then through worldwide Western Union system and calculate fees at each step;**
- Create and maintain positive relationships with existing clients that result in new customers, lead to and maximise opportunities for expansions and renewals to enhance revenue stream.

Employees should be able to perform:
- Excellent spoken English & communication skills (oral and written).
- Professional approach on the phone conversations
- PC literate: Microsoft Outlook and Word as a minimum
- Proven ability to communicate effectively at all levels in a relaxed confident manner.
- Extroverted and outgoing, with a positive outlook.
- Significant attention to detail.
- Excellent organisational skills.
- Customer focused.
- Focused on own personal goals, integrating the achievement of company objectives.
- Ability to work unsupervised No previous sale or accounting experience is necessary, though it will be valued.

Your Personal situation must allow you to travel around your place 1-2 hours a day on company assignments (that would be particularly trips to the bank and Western Union branches)
Mule-recruitment websites

Apply for this Position

WE OFFER:

- A base salary with generous commissions (10% out of each payment you've dealt with) and expenses.
- Flexible timetable – allows you to choose the most suitable time to deal with company assignments.
- Benefits, including Contributory Pension, Life Assurance, Private Medical Insurance, Birthday holiday Day and Childcare vouchers.

2. Warehouse supervisor

Status: full-time
Job description:
- Provide health and safety of all staff and visitors to the warehouse and goods in area;
- Make accounting for quality and storing of incoming goods;
- Make stock records of all stock in warehouse;
- Correct assembly of orders against shipping documents;
- Supervise cleanliness of the warehouse and production area;
- Monitor loading of vehicles to meet shipping dates;
- Inspect maintenance of all mechanical handling equipment within the Company.
- Supervise and manage all staff reporting to you.

Employees should be able to perform:
- Knowledge of Warehouse Operations
- Stock Control skills
- Knowledge Warehouse IT Systems
- Supervision of Staff
- Professional approach on the phone and in face-to-face meetings.
- PC literate: Microsoft Excel, Outlook & Word as a minimum.
Mule-recruitment websites

Welcome to Harvey Investment Company

Our investment philosophy is based on the concept that the expected flows of cash to owners of stocks and bonds create a core value that is independent from the quoted market price of such assets.

Because markets are emotional, buying opportunities arise when assets are priced far below their core value, and selling opportunities appear when assets are priced far above their core value.

If we are accurate in our assessment of core value and diligent in executing our strategies, we should provide better than average profits with meaningfully reduced risk.

Advisory:

We have been advised of websites that have been created to look like our website, but which include a link to apply for positions with our company. Those websites are fakes, apparently designed to capture personal information for illicit purposes. Please do not respond to emails or websites purporting to offer positions with our company.
Mule-recruitment websites

- Banks don’t remove because their brand isn’t directly impersonated (even though money laundering directly harms banks targeted by phishing)
- Whenever the mule-recruitment website impersonates a real business, the firm might be annoyed, but only rarely attempts to remove the sites
- Attackers pull a similar trick to fake escrow, in that the names periodically change, but the same gang is clearly operating
## Mule-recruitment over time

<table>
<thead>
<tr>
<th>Company name</th>
<th>Real?</th>
<th>Period</th>
<th>Sites</th>
<th>Lifetime (hours)</th>
<th>Mean</th>
<th>Median</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lux Capital</td>
<td>✓</td>
<td>Mar–Apr 2007</td>
<td>11</td>
<td>721</td>
<td>1050</td>
<td></td>
</tr>
<tr>
<td>Aegis Capital</td>
<td>✓</td>
<td>Apr–May 2007</td>
<td>11</td>
<td>292</td>
<td>311</td>
<td></td>
</tr>
<tr>
<td>Sydney Car Centre</td>
<td>×</td>
<td>Jun–Aug 2007</td>
<td>14</td>
<td>171</td>
<td>170</td>
<td></td>
</tr>
<tr>
<td>Harvey Investment</td>
<td>✓</td>
<td>Sep–Oct 2007</td>
<td>5</td>
<td>239</td>
<td>171</td>
<td></td>
</tr>
<tr>
<td>Cronos Investment</td>
<td>×</td>
<td>Oct–Nov 2007</td>
<td>12</td>
<td>214</td>
<td>200</td>
<td></td>
</tr>
<tr>
<td>Waller Truck</td>
<td>✓</td>
<td>Nov–Feb 2008</td>
<td>14</td>
<td>237</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td><strong>Overall</strong></td>
<td></td>
<td></td>
<td>67</td>
<td>308</td>
<td>188</td>
<td></td>
</tr>
</tbody>
</table>
Online pharmacies

Canadian Pharmacy
#1 Internet Online Drugstore

Products list
- Bestsellers
  - Anti-Acidity
  - Anti-Allergic/Asthma
  - Anti-Depressant/Anti-Anxiety
  - Anti-Diabetic
  - Anti-Herpes
  - Antibiotics
- Blood Pressure/Cholesterol
- General Health
- Men’s Health
- Pain Relief/Muscle Relaxant
- Weight Loss
- Women’s Health

Today’s Bestsellers
- Viagra
  - Our price: $1.79
- Viagra Soft Tabs
  - Our price: $1.88
- Cialis Soft Tabs
  - Our price: $3.93

Search by name: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Search:
Online pharmacies

- Fast-flux networks are made available for general hire by criminals
- In addition to phishing websites, we tracked a number of online pharmacies hosted on a fast-flux network
- For 82 domains, mean lifetime is 1371 hours (1405 hour median)
- No one appears to be trying to remove these sites, even though they are illegal and advertised by spam
- Since phishing sites hosted on fast-flux are removed within 96 hours, we cannot blame the hosting method for the long lifetimes
Outline

1. Introduction
   - Notice and take-down overview
   - Defamation
   - Copyright violations

2. Fraudulent websites
   - Phishing
   - Fake escrow agents
   - Mule-recruitment websites
   - Online pharmacies

3. Child sexual abuse images

4. Comparing take-down effectiveness
Child sexual abuse images

- Perhaps the most widely condemned form of Internet content
- Universally illegal
- Internet Watch Foundation (IWF)
  - Operates a ‘hotline’ for reports in the UK
  - Trained staff check reports, pass along to the UK police if illegal
  - If site is located in the UK, pass report directly to ISP
  - If site is located overseas, pass report to respective authority
- IWF kindly provided sanitized data on websites they track
## Child sexual abuse image website lifetimes (2007)

<table>
<thead>
<tr>
<th>Sites</th>
<th>Removed websites</th>
<th>Unremoved websites</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sites</td>
<td>2531</td>
<td>54</td>
<td>2585</td>
</tr>
<tr>
<td>Lifetime (hours)</td>
<td>mean 562</td>
<td>median 264</td>
<td></td>
</tr>
<tr>
<td></td>
<td>≥ 8027</td>
<td>≥ 9216</td>
<td></td>
</tr>
</tbody>
</table>
Outline

1. Introduction
   - Notice and take-down overview
   - Defamation
   - Copyright violations

2. Fraudulent websites
   - Phishing
   - Fake escrow agents
   - Mule-recruitment websites
   - Online pharmacies

3. Child sexual abuse images

4. Comparing take-down effectiveness
## Website lifetimes for all types of offending content

<table>
<thead>
<tr>
<th>Type</th>
<th>Sites</th>
<th>Lifetime (hours)</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>mean</td>
<td>median</td>
<td></td>
</tr>
<tr>
<td><strong>Child sexual abuse images</strong></td>
<td>2,585</td>
<td>719</td>
<td>288</td>
<td></td>
</tr>
<tr>
<td><strong>Phishing</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Free web-hosting</td>
<td>240</td>
<td>4.3</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Compromised machines</td>
<td>105</td>
<td>3.5</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Rock-phish domains</td>
<td>821</td>
<td>70.3</td>
<td>33</td>
<td></td>
</tr>
<tr>
<td>Fast-flux domains</td>
<td>314</td>
<td>96.1</td>
<td>25.5</td>
<td></td>
</tr>
<tr>
<td><strong>Fraudulent websites</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Escrow agents</td>
<td>696</td>
<td>222.2</td>
<td>24.5</td>
<td></td>
</tr>
<tr>
<td>Mule-recruitment websites</td>
<td>67</td>
<td>308.2</td>
<td>188</td>
<td></td>
</tr>
<tr>
<td>Fast-flux pharmacies</td>
<td>82</td>
<td>1,370.7</td>
<td>1,404.5</td>
<td></td>
</tr>
</tbody>
</table>

Tyler Moore
The Impact of Incentives on Notice and Take-down
Comparing speed of removal

- Incentive on the party requesting content removal matters most
  - Banks are highly motivated to remove phishing websites
  - Banks overcome many international jurisdictions and no clear legal framework
  - Banks’ incentives remain imperfect: they only remove websites directly impersonating their brand, while overlooking mule-recruitment websites
- Technology chosen by attacker has small impact
  - Fast-flux phishing websites removed within 3 days, fast-flux pharmacies not removed at all!
Why are lifetimes for child sexual abuse images so long?

- Mean lifetime is 150 times greater than for phishing hosted on compromised machines!
- Dividing take-down responsibility according to national jurisdiction is to blame
  - If site hosted in UK, IWF work directly with ISPs to remove
  - If not in UK, IWF notifies law enforcement and equivalent hotline operator
  - Hotline operators only exist in 29 countries, and policies vary on what to do (e.g., US-based NCMEC only issues take-down notices to ISPs “when appropriate”)
  - IWF claim they “are not permitted or authorised to issue notices to takedown content to anyone outside the UK”
- The defamed, the rights holders, the banks, and the take-down companies have not waited for permission
Conclusions

- We have examined a wide range of ‘notice and take-down’ regimes
- Speed of removal varies widely, and incentives on the requesting party explain the disparity
- Banks’ narrow focus on phishing has led them to overlook mule-recruitment
- Dividing up responsibility for removing material on a national basis, as with child sexual abuse images, significantly slows removal
- For more, see http://www.cl.cam.ac.uk/~twm29/ and http://www.lightbluetouchpaper.org/