Registrar Abuse Contacts

Dave Piscitello
ICANN SSAC
### Typical Phishing Domain Takedown

(Applies to most malicious domains)

<table>
<thead>
<tr>
<th>Hours 0-1</th>
<th>Phisher: Registers domain with Registrar</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phisher:</td>
<td>Creates phish site</td>
</tr>
<tr>
<td>Phisher:</td>
<td>Creates and sends phish email</td>
</tr>
<tr>
<td>Consumer:</td>
<td>Receives email</td>
</tr>
<tr>
<td>Anti-phishing</td>
<td>or Brand Owner: Identifies site,</td>
</tr>
<tr>
<td>service provider</td>
<td>investigates, and initiates shut down</td>
</tr>
<tr>
<td>or Brand Owner:</td>
<td>procedures</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hours 1-12</th>
<th>Anti-phishing service provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phisher:</td>
<td>or Brand Owner: Disables site by</td>
</tr>
<tr>
<td></td>
<td>contacting ISP, Registrar, or Site Owner</td>
</tr>
</tbody>
</table>

| Days 3+         | Consumer: Loses an average $1,244         |
|-----------------| (usually days after credentials stolen)   |
|                 | Law Enforcement: Starts investigation     |
|                 | (usually weeks later)                     |

How do interveners know whom to contact?

Graphic Courtesy of APWG
Sponsoring Registrar

• Interveners, LEAs, others *identify* the sponsoring registrar from Whois

• Issues:
  – Where do I find contact information for the sponsoring registrar?
  – Does the contact information I find lead me to someone who can handle abuse claims?
Sources for Registrar Contacts

• Visit the registrar’s web site
• Visit ICANN’s published list of registrar contacts, http://www.internic.net/regist.html
• Ask a colleague, ask a mail list, …
• Issue

Each failure to locate a registrar abuse point of contact extends the duration of an attack
Can you help me?

• Registrars publish information for many PoCs
  – Registrars publish contact information voluntarily
• Certain published PoCs
  – contain inaccurate or incomplete information
  – are not available 24 x 7
  – are unable to handle abuse or criminal complaints
  – are unable to escalate complaints
• Issue revisited
  – Each successive failure to locate a registrar abuse point of contact extends the duration of an attack
Can we do better?

- Ideal response times for phishing attacks are measured in hours
- Delays introduced while attempting to contact a registrar or finding the right PoC in the registrar are often measured in hours
- Can we reduce the delay?
Recommendations

• Each registrar should provide an abuse point of contact
  – Contacted party should be effective and responsive
  – Contacted party should provide complainants with a well-defined, auditable way to track abuse complaints

• Registrars should publish abuse contact information
  – List prominently on registrar web site
  – List prominently on ICANN web site

• Abuse contact information should be
  – Consistent with other registration contact records
  – Available in machine-readable format
  – Periodically checked for accuracy by ICANN