Tackling “phishing”

Dr Richard Clayton
(joint work with Tyler Moore)
The Effect of Scale: “Phishing”

• Punter receives email from their bank indicating their details needs refreshing

• URL looks convincing
  [http://www.mybank.com&account@107990442]

• Website looks convincing
  – usually copied from the real thing!

• Currently sites are usually too greedy & punters smell a rat. This will change
The Effect of Scale: “Phishing”

- Punter receives email from their bank indicating their details needs refreshing
- URL still looks convincing
- Website looks convincing
  – usually copied from the real thing!
- Multi-billion dollar losses occurring
  – risk that confidence in online banking will falter
Countermeasures

• Security markings within web-browsers
  – experiments show these are almost useless

• Two-factor authentication
  – expensive, can fail – but attackers go elsewhere

• Website take-down
  – industry says “within hours”, but we beg to differ

• Back office controls on transfers
  – seems to be main differentiator for losses
“Rock-phish” gang

• Distinctive URL style
  
  http://session9999.bank.com.lof80.info/signon/
  – end-users do not understand URL structure
  – variations help to evade email spam filters
  – domains are not trademarks, to slow down removal
  – attacking multiple banks in parallel

• Compromised machines run a proxy
  – robust against proxy removal & server is hidden
  – “fast-flux” means new address every 20 minutes
<table>
<thead>
<tr>
<th>Phishing website lifetimes (hours)</th>
<th># sites (8 weeks)</th>
<th>Mean lifetime</th>
<th>Median lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-rock</td>
<td>1695</td>
<td>62</td>
<td>20</td>
</tr>
<tr>
<td>Rock-phish domains</td>
<td>421</td>
<td>95</td>
<td>55</td>
</tr>
<tr>
<td>Fast-flux rock-phish domains</td>
<td>72</td>
<td>252</td>
<td>114</td>
</tr>
<tr>
<td>Rock-phish IP addresses</td>
<td>125</td>
<td>172</td>
<td>26</td>
</tr>
<tr>
<td>Fast-flux rock-phish IP addresses</td>
<td>4287</td>
<td>139</td>
<td>18</td>
</tr>
</tbody>
</table>
The numbers game

- Feb-Apr 2007: 1,707 phishing websites, 419 rock-phish domains and 67 fast-flux domains…
- PhishTank has 18,260 rock-phish reports, 1,803 fast-flux reports and 15,030 non-rock reports
  – some were dead by the time we looked, but many were duplicate entries or irrelevant variations
- Large numbers suit the security industry, community activists, law enforcement seeking excuses to ignore the problem…
Banks attacked (by non-rock-phish sites)

- PayPal: 23.8%
- eBay: 15.3%
- Bank of America: 12.1%
- Wachovia: 7.6%
- Wells Fargo: 3.3%
- etc etc etc

120 attacked in total
50 had just one attack
Some banks take-down faster…
Vacancies ............................................................

ENGINEERING MANAGER

Job description:

As an Engineering Manager you will be responsible for managing a portfolio of car maintenance contracts, maximizing customer satisfaction, and ensuring delivery of quality services while achieving set goals through effective management & coordination of personnel, equipment & facility resources, and employee training & development.

Primary responsibilities:

- Responsible for ensuring delivery of quality services and customer satisfaction;
- Develop long-term relationships with clients to ensure open-line of communication;
- Schedule car breakdown crews and conduct inspections to evaluate services performed;
- Responsible for monitoring operation expenses. Review financial reports & seek avenues to improve the branch’s bottom line;
- Develop and coordinate plans for the efficient use of personnel and resources.

Requirements:

- Experience with Windows, MS Office, Unix, SQL;
- Engineering Management System experience and understanding of basic networking;
- Excellent Customer Service skills;
- Assist in diagnosing and resolving car condition;
- Must be a good problem solver and have excellent written and oral communication skills;
- Excellent interpersonal skills and the ability to work as a unified team member.
REGIONAL ASSISTANT

Job description:

A regional assistant is a part time position, which will require only about 1-2 free hours a day from you. You will be responsible for dealing with the payments for the orders from our regional customers and fastening the process of payment delivery to the suppliers by means of Western Union. The peculiarity of the position is that your principal salary will be coming out of the fee that you get from each payment you dealt with (Net 10%).

Primary responsibilities:

- Communicate closely with the head office;
- Be available to receive 2-3 payments on your bank account from the customers every week;
- Make calculations regarding every transaction;
- Withdraw the funds from the bank account (less your 10% fee);
- Make transactions via Western Union to the suppliers;
- Inform the head office about every payment received and dealt with at the earliest convenience.

Requirements:

- Availability of a bank account;
- Excellent communication skills;
- Computer literacy;
- Excellent calculation skills;
- Industrious & goal-oriented.
“Mule” recruitment

• High proportion of spam devoted to recruitment shows that this is a significant bottleneck

• Aegis, Lux Capital, Sydney Car Centre, etc, etc
  – mixture of real firms and invented ones
  – some “fast-flux” hosting involved

• Only the vigilantes are taking these down
  – viz: amateur activists; usually objecting to spam
  – the impersonated are clueless and/or unmotivated
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.
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 site takedown is slow!

<table>
<thead>
<tr>
<th>Mule website lifetimes (hours)</th>
<th># domains</th>
<th>Mean lifetime</th>
<th>Median lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lux Capital</td>
<td>10</td>
<td>751</td>
<td>1058</td>
</tr>
<tr>
<td>Aegis Capital Group</td>
<td>11</td>
<td>292</td>
<td>311</td>
</tr>
<tr>
<td>Sydney Car Centre</td>
<td>17</td>
<td>182</td>
<td>135</td>
</tr>
<tr>
<td>Harvey Investments</td>
<td>-</td>
<td>ongoing</td>
<td>-</td>
</tr>
</tbody>
</table>
Whose problem is it?

• Removing mule recruitment sites is a problem for the banking INDUSTRY
• But expertise for removal resides within banks, or must be purchased from brand-protection companies ($400/site or more)
• Why should you bother to take down sites when you’re not currently their target?
Summary

• Back-end controls prevent phishing losses
  – but “mules” can appear to legitimise transactions

• Phishing website takedown is variable
  – 10 hours to 150 hours

• Mule recruitment website takedown is slow
  – 180 hours or more (easier to measure in weeks!)

• Industry needs to do more collectively, and
  put further pressure on an obvious bottleneck
Tackling “phishing”

BLOG: http://www.lightbluetouchpaper.org/

http://www.cl.cam.ac.uk/~rnc1/
http://www.cl.cam.ac.uk/~twm29/

http://www.cl.cam.ac.uk/~rnc1/weis07phishing.pdf