Anti-Phishing Working Group

www.antiphishing.org

Fall 2008 Phishing Update
ICANN – ccNSO
Cairo, Egypt, November 5, 2008

Rod Rasmussen
Co-Chair Internet Policy Committee of the APWG
President & CTO, Internet Identity

Dave Piscitello
Senior Security Technologist, SSAC
Topics

• Phish site education landing page
• New registrar phishing attacks
• APWG 1H 2008 phishing by TLD study results
• Live example - Venezuela
• Registry suspension plan status
• Registrar Best Practices document
Everything is Connected

Frauds

Spam

Phishing

Botnets

Malware

DDoS

Child Pornography

Mule Recruiting

Click Fraud
Phish Education Page: The Goal

Consumer is educated at the “most teachable moment” – immediately after having been fooled by a phishing communication
How it works…

1. Investigators determine that a domain or URL is a phishing page
2. Offending page is taken out of service
3. Operators modify DNS or hosting server so that domain/URL resolves to Phishing education page
4. All would-be victims are protected and provided with a learning opportunity
WARNING!

The web page you tried to visit might have been trying to steal your personal information. That page was removed after being identified as a "phishing" web page. A phishing web page tricks people out of bank account information, passwords and other confidential information.

How You Were Tricked

This email is from my bank and is asking me to update my information. I better click on the link and update it.

STOP! Don’t fall for scam email.

How to Help Protect Yourself

1. Don’t trust links in an email.
   DANGER! http://www.amazon.com/update

2. Never give out personal information upon email request.
   DANGER! Name: Jane Smith
   Credit Card: 1234 5678 9101 1212

3. Look carefully at the web address.
   http://www.amazon.com

4. Type the real website address into a web browser.
   http://www.amazon.com

5. Don’t call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement.

6. Don’t open unexpected email attachments or instant message unload links.

My Inbox

From: service@Wombank.com
Dear Jane,
Your account will be suspended if you do not update your information.
http://www.Wombank.com/update

For Customer Service call:
1-800-xxx-xxx

My Inbox

Here is the updated document attachment
Text Version of the Page

Warning!

The web page you tried to visit might have been trying to steal your personal information. The link you clicked to get here was probably created by con artists.

That page was removed after being identified as a “phishing” web page. A phishing web page is created to trick people out of bank account information, passwords and other confidential information.

Help Protect Yourself from Identity Theft

- Don't trust 'urgent' demands for personal information such as passwords in email or in instant messages.
  > STOP. Think. Avoid being rushed into giving up secrets or personal information you will later regret giving away.
- Don't trust links in email or in instant messages. They can lead to viruses and infect your computer.
  > MANUALLY TYPE the URLs for websites you need to visit, or use bookmarks you have created.
- Don't trust company telephone numbers in email or in instant messages.
  > LOOK UP telephone numbers using an established source. Use a telephone directory, a paper account statement or the telephone numbers on the back of your ATM cards and credit cards.
- Don't trust unexpected email attachments or instant message download links.
  > SCAN all attachments for viruses even in expected emails from friends and colleagues.

Legal Disclaimer

- PLEASE NOTE: The APWG, CMU’s Supporting Trust Decisions Project and any cooperating service providers have provided this message as a public service, based upon information that the URL you were seeking has been involved in a phishing or malware exploit. There is no guarantee that you have not been phished or exposed to malware from this URL you were seeking, or previously. This is not a complete list of steps that may be taken to avoid phishing or malware. For example, refer to the Anti-Phishing Working Group (APWG) website for a list of tips to avoid phishing and malware.

Text and image-rich pages will be translated into many languages

Anti-Phishing Working Group
Committed to wiping out Internet scams and fraud
Questions for ccTLD Registries

• Can we enlist the help of domain registries to help recruit and support registrars to implement use of the landing page?
• Will you adopt usage yourself if your model allows it?
• Can you provide a standardized DNS location?
• Can you volunteer to assist in translation effort?
Phishing of Registrars/Registries

- ICANN phished after Paris meeting
- SOPHISTICATED attack launched this week
- eNom and Network Solutions targeted so far
- Threat REMAINS one of the largest potential disasters for the Internet and ICANN
  - Take over of a Financial Institution’s domain portfolio through registrars’ domain management systems
  - Majority of accounts still protected by username/password only
Phishing Lures

From: eNom Tech Support <info2@enom.com>
Subject: Your domain must be deleted today!
Date: October 31, 2008
To: info@*

Dear user,

On Sat, 1 Nov 2008

We have received a notification from ICANN that the domain name [redacted] is set to expire on Wednesday, October 31, 2008. If the domain name is not renewed by that date, it will be removed from the ICANN database.

The contact information for the domain which displayed in the Whois database was indeed invalid. On Sat, 1 Nov 2008 02:16:27 +0100 we sent a notice to you at the admin.tech contact email address and the account email address informing you of invalid data in breach of the domain registration agreement.

We have been unable to contact the current domain owner to verify the contact information. We have therefore decided to remove the domain from the ICANN database.

Please verify your contact information at http://www.enom.com.

If you find any invalid contact information for this domain please respond to this email with evidence of the specific contact information you have found to be invalid on the Whois record for the domain name. Examples would be a bounced email or returned postal mail. If you have a bounced email, please attach or forward with your reply or in the case of returned postal mail, scan the returned letter and attach to your email reply or please send it to:

Attn: Domain Services 14455 N Hayden Rd Suite 219 Scottsdale, AZ 85260

http://www.enom.com.ssl45.mobi/

http://www.enom.com.sys49.mobi/

http://www.networksolutions.com.sys49.mobi/

http://www.enom.com.ssl45.mobi/

http://www.enom.com.sys49.mobi/

http://www.enom.com.ssl45.mobi/

http://www.enom.com.sys49.mobi/

http://www.enom.com.ssl45.mobi/

http://www.enom.com.sys49.mobi/

http://www.enom.com.ssl45.mobi/

http://www.enom.com.sys49.mobi/

http://www.enom.com.ssl45.mobi/

http://www.enom.com.sys49.mobi/

http://www.enom.com.ssl45.mobi/

http://www.enom.com.sys49.mobi/

http://www.enom.com.ssl45.mobi/

http://www.enom.com.sys49.mobi/

http://www.enom.com.ssl45.mobi/

http://www.enom.com.sys49.mobi/
Phishing Sites
Sophisticated attack vector

- The lures use many anticipated registrar messages (domain expires, whois update, errors)

- Fast-Flux based attack used 10 IPs at once on various domains

- “Man on the side” data grabbing – unique attack
  - Use real code they scraped from the registrar site and use it as-is on their site
  - Use Javascript for a “simultaneous” request for a URL

- Data you enter into the phishing site actually posts to the real site too
Global Phishing Survey
1H2008

Greg Aaron

Rod Rasmussen

Data Set

• Comprehensive sources: APWG, phishing feeds, private sources, honeypots

• Millions of phishing URLs $\rightarrow$ small number of domain names

• Total of 167,638,848 domain names in the TLDs we have stats for. Accounts for ~99% of domain names in the world.
  – .cc, .to, .tv, .ph, .nu would be nice to get too!
<table>
<thead>
<tr>
<th>Overall Stats</th>
<th>1H2008</th>
<th>2H2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing on unique domain names:</td>
<td>26,678</td>
<td>28,818</td>
</tr>
<tr>
<td>IP-based phish (unique IPs):</td>
<td>3,389</td>
<td>5,217</td>
</tr>
<tr>
<td>TLDs phished on:</td>
<td>155</td>
<td>145</td>
</tr>
<tr>
<td>“Attacks”:</td>
<td>&gt;47,342</td>
<td></td>
</tr>
<tr>
<td>IDN domains:</td>
<td>52</td>
<td>10</td>
</tr>
</tbody>
</table>
Phishing by TLD: Scores

- Metric: “Phishing domains per 10,000”
- Measures prevalence of phishing in a TLD
- Median score: 2.3
- .COM score: 1.6
- Scores skew higher for smaller TLDs
# Top 10 Phishing TLDs by Score

*(minimum 30,000 domains and 25 phish)*

<table>
<thead>
<tr>
<th>Rank</th>
<th>TLD</th>
<th>TLD Location</th>
<th># Unique Phishing attacks 1H2008</th>
<th>Unique Domain Names used for phishing 1H2008</th>
<th>Domains in registry in May 2008</th>
<th>Score: Phish per 10,000 domains 1H2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>hk</td>
<td>Hong Kong</td>
<td>2,278</td>
<td>516</td>
<td>160,336</td>
<td>32.2</td>
</tr>
<tr>
<td>2</td>
<td>th</td>
<td>Thailand</td>
<td>154</td>
<td>84</td>
<td>35,757</td>
<td>23.5</td>
</tr>
<tr>
<td>3</td>
<td>bz</td>
<td>Belize</td>
<td>52</td>
<td>43</td>
<td>43,216</td>
<td>10.0</td>
</tr>
<tr>
<td>4</td>
<td>ve</td>
<td>Venezuela</td>
<td>86</td>
<td>71</td>
<td>75,000</td>
<td>9.5</td>
</tr>
<tr>
<td>5</td>
<td>cl</td>
<td>Chile</td>
<td>274</td>
<td>128</td>
<td>212,153</td>
<td>6.0</td>
</tr>
<tr>
<td>6</td>
<td>ro</td>
<td>Romania</td>
<td>184</td>
<td>142</td>
<td>284,700</td>
<td>5.0</td>
</tr>
<tr>
<td>7</td>
<td>li</td>
<td>Liechtenstein</td>
<td>97</td>
<td>26</td>
<td>59,546</td>
<td>4.4</td>
</tr>
<tr>
<td>8</td>
<td>name</td>
<td>sponsored TLD</td>
<td>331</td>
<td>126</td>
<td>289,343</td>
<td>4.4</td>
</tr>
<tr>
<td>9</td>
<td>tw</td>
<td>Taiwan</td>
<td>319</td>
<td>145</td>
<td>385,500</td>
<td>3.8</td>
</tr>
<tr>
<td>10</td>
<td>kr</td>
<td>Korea</td>
<td>697</td>
<td>345</td>
<td>945,000</td>
<td>3.7</td>
</tr>
</tbody>
</table>
Phishing by Uptime

• For 2008, gathering “live” times for phish
  – Automated monitoring of phishing sites
  – Check site status several times per hour. Site must stay down for at least 1 hour.

• Average and Median live times
  – Median is better barometer of how overall efforts are going
  – A few outliers that last weeks can vastly skew averages
  – Some stark examples between TLDs

• Overall stats:
  – All 51,500 attacks: median 19.5 hours, average 49.5 hours
  – 47,300 domain-based attacks: median 19 hours, average 49 hours
  – 4,200 IP-based attacks: median 25.5 hours, average 59.5 hours
## 1H 2008 GTLD Uptimes

<table>
<thead>
<tr>
<th>TLD</th>
<th>Ave. Uptime Hours</th>
<th>Median Uptime Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>.com</td>
<td>56:06</td>
<td>21:17</td>
</tr>
<tr>
<td>.net</td>
<td>48:09</td>
<td>20:51</td>
</tr>
<tr>
<td>.org</td>
<td>51:38</td>
<td>20:22</td>
</tr>
<tr>
<td>.info</td>
<td>25:13</td>
<td>15:24</td>
</tr>
<tr>
<td>.biz</td>
<td>38:35</td>
<td>15:05</td>
</tr>
</tbody>
</table>
Subdomain Services

- `<customer_term>..<service_provider_sld>.TLD`
- 4500+ subdomain sites/accounts on 274 unique second-level domains
- If we counted these as “domain names,” they would represent 9.5% of all domains
- For some TLDs, can greatly increase attack count
- Examples:
  - 379 phish on pochta.ru, 316 on land.ru, 251 on smtp.ru
  - 262 phish on ns8-wistee.fr, 250 on free.fr
  - 256 on 9k.com, 255 on altervista.org
- Up-times
  - Average: 45 hours, Median: 17 hours
  - Slightly better than overall numbers
## Top 20 Subdomain Phishing Attacks

<table>
<thead>
<tr>
<th></th>
<th>Domain</th>
<th>Phish Sites</th>
<th>Domain Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>pochta.ru</td>
<td>379</td>
<td>Pochta.ru</td>
</tr>
<tr>
<td>2</td>
<td>land.ru</td>
<td>316</td>
<td>Pochta.ru</td>
</tr>
<tr>
<td>3</td>
<td>ns8-wistee.fr</td>
<td>262</td>
<td>wistee.fr</td>
</tr>
<tr>
<td>4</td>
<td>9k.com</td>
<td>256</td>
<td>9k.com</td>
</tr>
<tr>
<td>5</td>
<td>alternista.org</td>
<td>255</td>
<td>alternista.org</td>
</tr>
<tr>
<td>6</td>
<td>smtp.ru</td>
<td>251</td>
<td>Pochta.ru</td>
</tr>
<tr>
<td>7</td>
<td>free.fr</td>
<td>250</td>
<td>free.fr</td>
</tr>
<tr>
<td>8</td>
<td>nm.ru</td>
<td>171</td>
<td>Pochta.ru</td>
</tr>
<tr>
<td>9</td>
<td>t35.com</td>
<td>142</td>
<td>t35.com</td>
</tr>
<tr>
<td>10</td>
<td>jexiste.fr</td>
<td>95</td>
<td>jexiste.fr</td>
</tr>
<tr>
<td>11</td>
<td>110mb.com</td>
<td>90</td>
<td>110mb.com</td>
</tr>
<tr>
<td>12</td>
<td>front.ru</td>
<td>82</td>
<td>Pochta.ru</td>
</tr>
<tr>
<td>13</td>
<td>krovatka.su</td>
<td>71</td>
<td>Pochta.ru</td>
</tr>
<tr>
<td>14</td>
<td>notlong.com</td>
<td>63</td>
<td>notlong.com</td>
</tr>
<tr>
<td>15</td>
<td>freeweb7.com</td>
<td>62</td>
<td>freeweb7.com</td>
</tr>
<tr>
<td>16</td>
<td>freehostia.com</td>
<td>60</td>
<td>freehostia.com</td>
</tr>
<tr>
<td>17</td>
<td>us.com</td>
<td>55</td>
<td>CentralNIC</td>
</tr>
<tr>
<td>18</td>
<td>de.com</td>
<td>45</td>
<td>CentralNIC</td>
</tr>
<tr>
<td>19</td>
<td>ifrance.com</td>
<td>44</td>
<td>ifrance.com</td>
</tr>
<tr>
<td>20</td>
<td>host.sk</td>
<td>40</td>
<td>host.sk</td>
</tr>
</tbody>
</table>
## Top 15 Phishing TLDs by Attack Score

<table>
<thead>
<tr>
<th>Rank</th>
<th>TLD</th>
<th>TLD Location</th>
<th># Unique Phishing attacks</th>
<th>Unique Domain Names used for phishing</th>
<th>Domains in registry in May 2008</th>
<th>Score: Phish per 10,000 domains</th>
<th>Score: Attacks per 10,000 domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>hk</td>
<td>Hong Kong</td>
<td>2,278</td>
<td>516</td>
<td>160,336</td>
<td>32.2</td>
<td>142.1</td>
</tr>
<tr>
<td>2</td>
<td>th</td>
<td>Thailand</td>
<td>154</td>
<td>84</td>
<td>35,757</td>
<td>23.5</td>
<td>43.1</td>
</tr>
<tr>
<td>3</td>
<td>su</td>
<td>Soviet Union</td>
<td>154</td>
<td>14</td>
<td>60,543</td>
<td>2.3</td>
<td>25.4</td>
</tr>
<tr>
<td>4</td>
<td>li</td>
<td>Liechtenstein</td>
<td>97</td>
<td>26</td>
<td>59,546</td>
<td>4.4</td>
<td>16.3</td>
</tr>
<tr>
<td>5</td>
<td>ru</td>
<td>Russia</td>
<td>1,907</td>
<td>362</td>
<td>1,427,928</td>
<td>2.5</td>
<td>13.4</td>
</tr>
<tr>
<td>6</td>
<td>cl</td>
<td>Chile</td>
<td>274</td>
<td>128</td>
<td>212,153</td>
<td>6.0</td>
<td>12.9</td>
</tr>
<tr>
<td>7</td>
<td>bz</td>
<td>Belize</td>
<td>52</td>
<td>43</td>
<td>43,216</td>
<td>10.0</td>
<td>12.0</td>
</tr>
<tr>
<td>8</td>
<td>ve</td>
<td>Venezuela</td>
<td>86</td>
<td>71</td>
<td>75,000</td>
<td>9.5</td>
<td>11.5</td>
</tr>
<tr>
<td>9</td>
<td>name</td>
<td>sponsored TLD</td>
<td>331</td>
<td>126</td>
<td>289,343</td>
<td>4.4</td>
<td>11.4</td>
</tr>
<tr>
<td>10</td>
<td>fr</td>
<td>France</td>
<td>1,236</td>
<td>107</td>
<td>1,128,776</td>
<td>0.9</td>
<td>10.9</td>
</tr>
<tr>
<td>11</td>
<td>es</td>
<td>Spain</td>
<td>883</td>
<td>333</td>
<td>970,580</td>
<td>3.4</td>
<td>9.1</td>
</tr>
<tr>
<td>12</td>
<td>be</td>
<td>Belgium</td>
<td>690</td>
<td>62</td>
<td>791,737</td>
<td>0.8</td>
<td>8.7</td>
</tr>
</tbody>
</table>
Some Conclusions

Phishers are always adjusting and experimenting
  – Moving from registrar to registrar, and TLD to TLD
  – Moving away from using IP-based phishing

Use of domain names for phishing remained flat.

Still very little use of IDNs for phishing

Registry anti-abuse programs have an effect.

Venezuela: a Live Lesson

• TLD: .VE
• Combined Registry/Registrar Model
• Open registration policy
• Partial governmental control
  – Ministry in charge has changed in last few months
  – Indirect relationship to national police
• Prior to summer 2008 – very little phishing
  – Several domains in Feb-April 2008 but then a lull
• July 2008, new attacks start with a few sites
  – Register suspect names with all 6 sub-TLD variants
  – Initial response is pretty swift
Venezuela: Problems arise

• Process quickly breaks-down as dozens of domains are registered
• Work with registry to help them understand issues
  – Provide information on recent experiences of other registries (.HK primarily)
  – Coordinate with LACTLD
• Start to require “police directive” for shut-down
• Registry then claims they can’t suspend obviously fraudulent domains at all
  – Phishers start registering domains in the name of Donald Trump and “Internet Identity”
  – Registry STILL won’t suspend even though the take-down service is the registrant!
Ouch!

VE Fraudulent Phishing Domains 2008

July  | August | September | October
0     | 100    | 200       | 1800
Venezuela: What happened?

• NIC caught completely unprepared
• Stuck to policy rather than practical realities
• Take-down times dragged out to 2 weeks
• Phishers saw this
  – Vastly increased registrations
  – Taunted them/us
• Slow, bureaucratic path to change policy and process
• We may have a fix now – still waiting to see
• Ecuador (.ec) appears to be next in line…
  – We are working with LACTLD to try to come up with policy that all NICs in their region can utilize
  – We can really use your support on this effort!
Accelerated Domain Suspension Plan for Registries: Update

- .Asia expressed interest in getting this done and in place after recent .asia based phish
- We’re a bit stuck
  - Accreditation agency to vet qualified interveners identified but will cost $$$
  - Interveners willing to pay, but need more bang for the buck
- So who else is willing to sign on to this idea?
  - Allows a registry to take active anti-abuse role within defined process and shared responsibility
  - Latest survey shows these efforts are effective
Registrar Best Practices

• **Goal:**
  – Cooperative effort between APWG and ICANN registrars
  – *Recommend* measures registrars can take to assist the anti-phishing community make the Internet safer for all

• **Focus:**
  – Evidence preservation (help LE catch the criminals)
    • What is useful? How to preserve? Who to provide to?
  – Registrant screening tips to identify fraud proactively
  – Phishing domain takedown assistance
  – Promote resources to help identify malicious activities

• Final version published at APWG site
Top Recommendations

1. Timely response to domain take-down requests by shutdown authorities and/or law enforcement
2. Proactively use available data to identify and shut-down malicious domains
3. Share fraudulent domain registration information with law-enforcement
4. Protect registrar customers from being phished
5. Prohibit/minimize use of Fast-Flux Domains
Other Recommendations

1. Investigate domain registrations/name servers related to known criminal activity (i.e. if you know one domain has fraudulent aspects, find and eliminate others with the same)

2. Gather data used in bogus registrations for “scoring” future registration attempts

3. Update Acceptable Use Policy/Service Agreement – Cover yourself so you can eliminate bogus domains anytime
APWG Contacts

- Website: http://www.antiphishing.org
- Phish Site Reporting: reportphishing@antiphishing.org
- Membership: membership@antiphishing.org
- e-mail
  - rod.rasmussen@internetidentity.com
  - Dave.piscitello@icann.org
Fall 2008 Phishing Update
ICANN – ccNSO
Cairo, Egypt, November 5, 2008

Rod Rasmussen
Co-Chair Internet Policy Committee of the APWG
President & CTO, Internet Identity

Dave Piscitello
Senior Security Technologist, SSAC

Anti-Phishing Working Group
www.antiphishing.org

Anti-Phishing Working Group
Committed to wiping out Internet scams and fraud