Domain Registration Abuse, Law Enforcement and Policy of WHOIS for .hk and .香港

Jonathan Shea
26 August 2011
Phishing and Spamvertising using ‘.hk’ (Received vs Suspended)
## Registration for Malicious Purpose

<table>
<thead>
<tr>
<th>Year</th>
<th>Phishing domains ever suspended</th>
<th>Spamvertising domains ever suspended</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>1,960</td>
<td>8,789</td>
</tr>
<tr>
<td>2008</td>
<td>503</td>
<td>104</td>
</tr>
<tr>
<td>2009</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>2010</td>
<td>29</td>
<td>0</td>
</tr>
<tr>
<td>2011 (until July)</td>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>

- There was a large number of malicious domain registrations in 2007 & 2008. We suspended a large number of domains as a result. Cyber-criminals therefore lost interest in using .hk domains.

- In 2009, we found a phisher holding a no. of .hk domain names. Though he was using only one of them for malicious purpose, we suspended all the domains under his name. This made the figure in 2009 relatively higher.

- Spamvertising here means the practice of sending email spam to advertise a website whose web address made up of a .hk domain. The websites usually are pornographic, pharmaceutical or gambling which are illegal businesses.
Registration for Malicious Purposes

Measures
• Identify malicious registration by reviewing data provided during application. If data is suspicious, request document to prove the applicant’s legal status before accepting the domain application.

• Already set up channel with Hong Kong Police, HKCERT to communicate, give professional advice and handle suspected cases.

• Registry oversees the responsiveness and readiness to take action of registrars closely to ensure registrars do not leave the problems unattended.

• Domain Registration Policy already included clauses giving right to registrars to take down .hl domain names when the registration is identified to be malicious.

• Registry also proactively reports statistics of phishing and spamvertising of .hk to media every year.
Law Enforcement related to Domain Abuse

• Currently there is no criminal law in Hong Kong specially for domain abuse.
• However if any persons gain access to computer with criminal or dishonest intent, he/she is committing a criminal offence.
• For some phishing cases on the Internet, the phishers committed an offence under Theft Ordinance.
• Law enforcement agency usually requests the registrar to suspend or cancel the domain or provide them with registration information for further investigation.
• Under the Personal Data (Privacy) Ordinance, personal data used in prevention and detection of crime are exempted from the data protection principle.
Repeated Applications for the Same .hk

• 20 days are allowed for applicants to pay and to provide documents (if required)
• Repeatedly applied for the same domain without making payment as a means to “block” others from registering the domain.
• Countering policy: if the same applicant does so more than twice within 6 months, we will withhold the domain from online application. Applicant shall write to us and provide payment before the applicant can apply for it. It is also on first-come, first-served basis.
• >400 .hk were held up because of the above measure. We observed >10 applicants engaged in repeated applications for the same domain names.
WHOIS Database for .hk /

- For individual domain registrations, we show only limited information which are also personal data, i.e. not more than the name and email address.
- Our domain registration policy granted us right to show the holder’s contact information on WHOIS.
- Domain holder has the responsibility to keep the contact information up to date.
- We have the right to cancel the domain registration if the holder intentionally provides false information.
Checking Correctness of WHOIS Information

- **Yearly Random Verification**
  - **In the Past:**
    - We randomly selected several hundred domains. Sent letter by post and emailed to ask them to provide documents (to prove their legal status) for verification. Only ~40% responded. We did not delete the rest because most of them were having an operating websites and businesses.
  - **In the Future:**
    - Will do eye-ball checking and identify abnormal applications e.g. registrant name = abcdefghijklmnopq, then request registrant / registrar to send document to prove its legal status. Stringent action will be taken if no response.
    - Request registrars to remind their customers at least once a year to keep their WHOIS information updated.
Multilingual WHOIS

- Currently customers must provide English Registrant Name
- Providing Chinese Registrant Name is only optional
- Address can be input in either English or Chinese
- Filling out Chinese address may create a problem for overseas complainants who may not be able to contact domain holder by mail for any purpose (e.g. before dispute settlement, legal proceeding etc.)
- We may consult stakeholders regarding kind of WHOIS data and language used in the future. Should also follow work done by IRD Group of ICANN
WHOIS for Organizational Type Domain

Domain Name: HKIRC.HK
Bundled Domain Name: 香港互聯網註冊.HK /
香港
Contract Version: HKDNR latest version
Domain Name Commencement Date: 04-05-2004
Expiry Date: 16-11-2014
Re-registration Status: Complete
Name of Registrar: HKDNR
Domain Status: Active

Registrant Contact Information
Holder Name(English): HONG KONG INTERNET REGISTRATION CORPORATION LIMITED
Holder name(Chinese): 香港互聯網註冊管理有限公司
Address: Unit 2002-2005, 20/F ING Tower, 308 Des Voeux Road Central, Sheung Wan, Hong Kong.
Country: HK
Email: jonathan.shea@hkdnr.hk

Administrative Contact Information
Given name: Jonathan
Family name: Shea
Contact Chinese Name:
Organization name(English): HONG KONG INTERNET REGISTRATION CORPORATION LTD.
Address: Unit 2002-2005, 20/F ING Tower, 308 Des Voeux Road Central, Sheung Wan, Hong Kong.
Country: HK
Phone:+852-23191313
Fax:+852-23192626
Email: jonathan.shea@hkdnr.hk
Account Name: HK1478901T

Technical Contact Information
Given name: Ben
Family name: Lee
Contact Chinese Name:
Organization name(English): HONG KONG INTERNET REGISTRATION CORPORATION LTD.
Address: Unit 2002-2005, 20/F ING Tower, 308 Des Voeux Road Central, Sheung Wan, Hong Kong.
Country: HK
Phone:+852-23191313
Fax:+852-23192626
Email: ben.lee@hkdnr.hk

Name Servers Information
Name Server 1: NS5.HKDNR.NET.HK
Name Server 2: NS6.HKDNR.NET.HK
WHOIS for Individual Type Domain

Domain Name: CHANDAIMAN.HK
Bundled Domain Name: 陳大文.香港
Contract Version: HKDNR latest version
Domain Name Commencement Date: 07-05-2004
Expiry Date: 15-05-2012
Re-registration Status: Complete
Name of Registrar: HKDNR Domain
Status: Active

Registrant Contact Information
Holder Name(English): CHAN DAI MAN
Holder Name(Chinese):
Email: dmchan@netvigator.com
Country: HK
Account Name: HK1482345T

Technical Contact Information
Given name: DAI MAN
Family name: CHAN
Contact Chinese Name:
Organization Name (English): BEST HOSTING LTD.

Name Servers Information
Name Server 1: NS5.HKDNR.NET.HK
Name Server 2: NS6.HKDNR.NET.HK
Thank you

Q & A