



H
K
I
R
C

Combat Phishing and Spamvertising using .hk Domains

Presented by Jonathan Shea

Chief Executive Officer

Hong Kong Internet Registration Corporation Limited

Hong Kong Domain Name Registration Company Limited

15 Jul 2008



.hk .edu.hk .idv.hk .com.hk .org.hk .net.hk .gov.hk .edu.hk .idv.hk .com.hk .org.hk .net.hk
.com.hk .org.hk .net.hk .gov.hk .edu.hk .idv.hk .com.hk .org.hk .net.hk .gov.hk .edu.hk .idv.



HKIRC

Agenda



- ❑ Introduction of HKIRC/HKDNR and .hk Domain
- ❑ Situation of Phishing and Spamvertising using .hk domains
- ❑ Process for Handling Phishing / Spamvertising
- ❑ Behavior of Criminals and Our Control Measures
- ❑ Difficulties Faced by Domain Registries/Registrars
- ❑ Collaboration of Domain Registries/Registrars with CERTs and Law Enforcement Agencies





HKIRC

Introduction of HKDNR/HKIRC

- HKDNR is an operating arm of HKIRC in .hk domain administration.
- HKDNR is a registry and a registrar (combination model) for .hk domain administration
- 165,324 .hk domain registrations as at 30 Jun 2008
- HKIRC set up since 2002. The first phishing domain was reported in Sept 2006.



HKDNR



H
K
I
R
C

Types of .hk Domains





What are Phishing and Spamvertizing?

Definitions

(Source: <http://en.wikipedia.org>)

- ❑ **Phishing** is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. eBay, PayPal and online banks are common targets. Phishing is typically carried out by email.
- ❑ **Spamvertizing** is the practice of sending E-mail spam, advertising a website. In this case, it is a portmanteau of the words "spam" and "advertising ". Spamvertizers insert links to their websites (typically, sites purporting to sell some commercial product). The links typically lead to pills, porn and poker sites.



HKDNR

RESTRICTED - NO COPYING

ALLOWED



Figure of Phishing and Spamvertizing on .hk domains in 2007

Report of Phishing

Month	No. of .hk domain reported for Phishing
Jan 2007	2
Feb 2007	21
Mar 2007	95
Apr 2007	243
May 2007	114
Jun 2007	234
Jul 2007	159
Aug 2007	294
Sep 2007	5
Oct 2007	139
Nov 2007	93
Dec 2007	278

Report of Spamvertizing

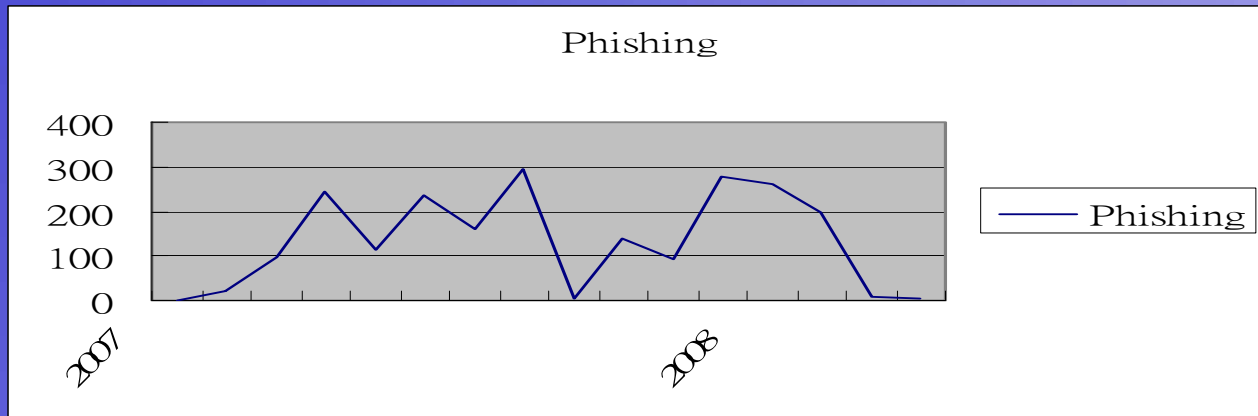
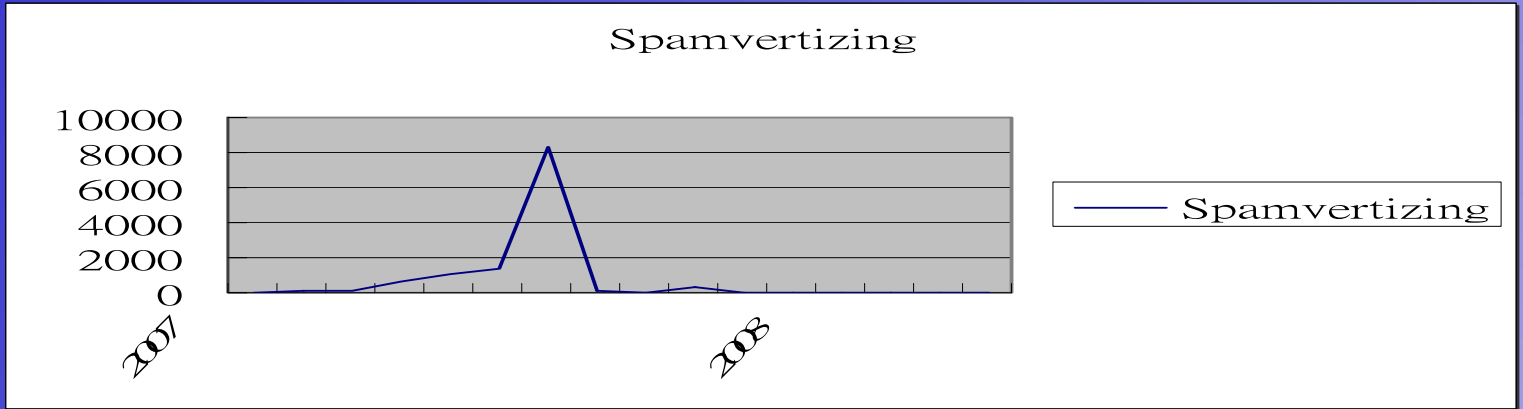
Month	No. of .hk domain reported for Spamvertizing
Jan 2007	35
Feb 2007	66
Mar 2007	105
Apr 2007	643
May 2007	1046
Jun 2007	1326
Jul 2007	1552 + 8321*
Aug 2007	71
Sep 2007	20
Oct 2007	299
Nov 2007	9
Dec 2007	33

* Reported by OFTA, some may overlap with reports already received by us



HKIRC

Phishing and Spamvertizing on .hk domains



HKDNR



Control Measures

Month	reported for Phishing (domain)	reported for spamvertizing (domain)
Dec 2006	2	7
Jan 2007	2	35
Feb 2007	21	66
Mar 2007	95	105
Apr 2007	243	643
May 2007	114	1046
Jun 2007	234	1326
Jul 2007	159	1552 + 8321
Aug 2007	294	71
Sep 2007	5	20
Oct 2007	139	299
Nov 2007	93	9
Dec 2007	278	33

Action in Feb 2007 and Before
Already amended registration agreement. Verified phishing domains were suspended on the same day (we worked on report from HK Police Force only)

Action in Mar and Apr 2007
1) HKCERT helped develop guideline to verify phishing domains. Identification of phishing domains became faster.

Action in Jun and Jul 2007
1) Restrict to accept only VBV / secure code ready credit cards
2) OFTA provides daily spamvertized list. >7,000 domains were suspended in Jul (completed on 20 Jul 07)

Action in Aug 2007
1) Daily monitoring of new registration with suspicious payment and registration pattern e.g. used lost card to settle payment etc.
2) Article posted on spamtracker.eu for our fighting against phishing and spamvertizing



Control Measures

Month	reported for Phishing (domain)	reported for spamvertising (domain)
Jan 2008	259	10
Feb 2008	200	1
Mar 2008	8	12*
Apr 2008	3	6*
May 2008	1	1*
Jun 2008	1*	7*

Action in Jan to Mar 2008

- 1) Increase frequency of domain suspension i.e. from 2 times to 3 times a day
- 2) Not accept credit cards that were used for phishing / spamvertising domains to use again

Mar 2008
Request documentary proofs for some new suspicious registration (including 2LD)

Apr to Jun 2008
After we request documentary proofs for suspicious application, we rec'd only a few reported cases. The reported spamvertising cases from Mar to Jun and the reported phishing case in June were false reports. In short, only 3 phishing domains were found.

* False Reports



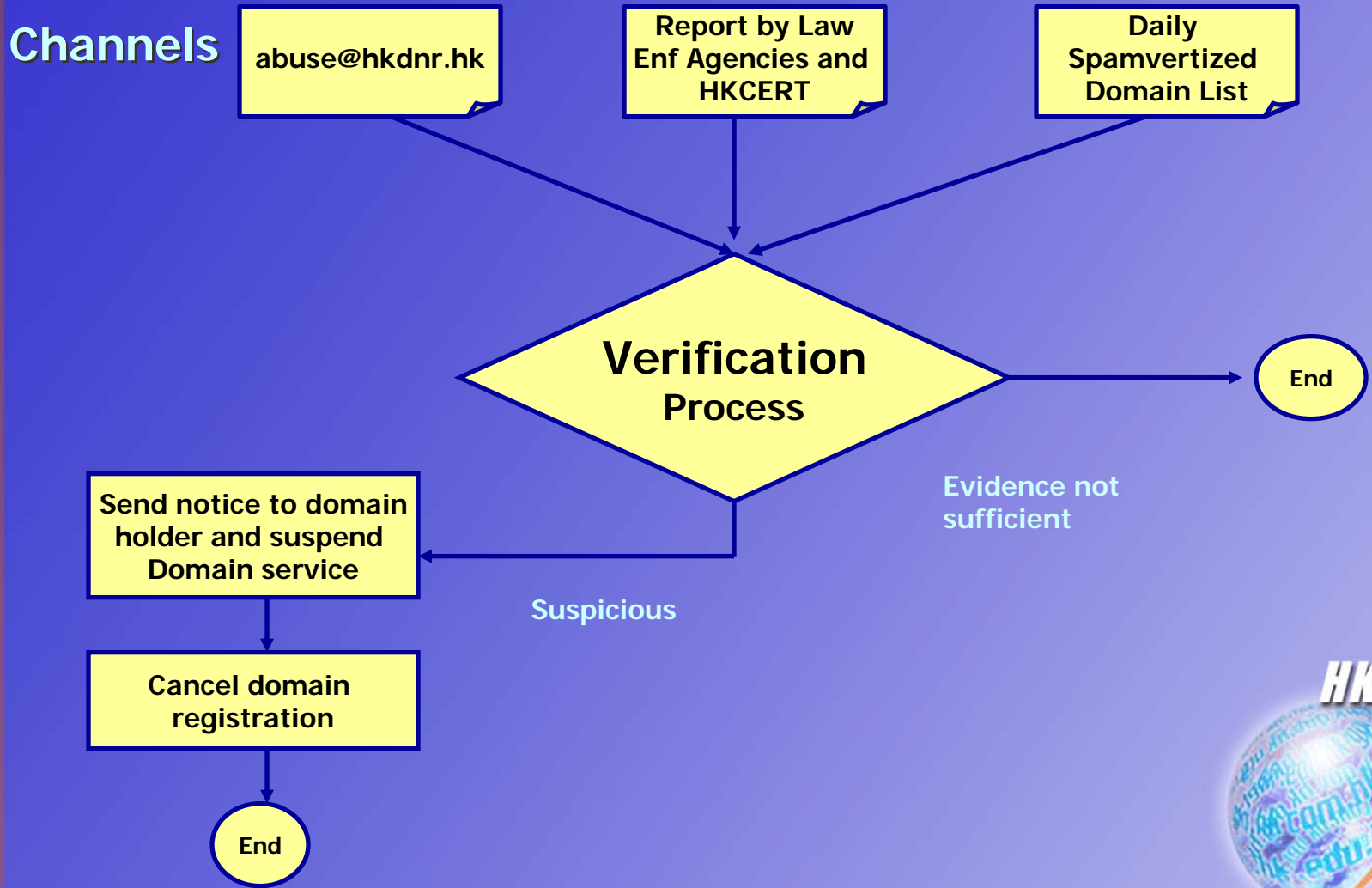
HKIRC

HKDNR



HKIRC

Process of Verification and Suspension





HKIRC

Objection Handling

- ❑ We have an objection handling procedure in place to handle objections for domain suspension due to phishing or spamvertizing.
- ❑ The opponent has to provide at least the identity proof and grant us right to send the proof to law enforcement agencies as needed before we consider the objection case.
- ❑ The procedure is formulated giving consideration to minimize the opportunity for bribery and conspiracy between individual employee and fraudster i.e. decision to re-activate domain involves at least 2 staff in different teams.



HKIRC

HKDNR

RESTRICTED - NO COPYING
ALLOWED



Common Difficulties Faced by Domain Registries/Registrars and How HKDNR coped with it

Common Difficulties Faced by Domain Registries/Registrars	What to be done by HKDNR
1) Do not have expertise to verify if the reported domain is a phishing / spamvertized domain	<ul style="list-style-type: none">❖ HKCERT and OFTA offered help in establishing our own verification guideline for phishing and spamvertizing❖ Closely monitor the registration pattern by phisher (give us more confidence to take action)❖ Have Objection Procedure in place
2) Have no right to cancel phishing domain	<ul style="list-style-type: none">❖ amend registration agreement so as to give more flexibility and right to take action
3) Too much domain registration barrier will hinder the use of domains	<ul style="list-style-type: none">❖ will be flexible to set barrier for a period of time when it is at CRISIS Level



H
K
I
R
C

Collaboration of Domain Registries / Registrars with CERTs and Law Enforcement Agencies



HKDNR

RESTRICTED - NO COPYING

ALLOWED



Collaboration of Domain Registries / Registrars with CERTs and Law Enforcement Agencies

- Domain Registries / Registrars have a part to play to fight against phishing / spamvertising in the battle field.
- A tank cannot fight the battle on its own. It needs intelligence, directions, investigations.....in order to achieve its mission.
- CERT provides information, experience, expertise...
- Law Enforcement Agencies provide information that Registries / Registrars may not be able to investigate on its own e.g. BOTNET case etc
- Registries / Registrars provide registration information that helps investigations by Law Enforcement Agencies





The Way Forward

- ❖ Like the real world, the cyberworld has both good and bad people. Criminals will not disappear overnight.
- ❖ Cyber-criminals are well organized, sophisticated and technically very competent. They are always looking for new ways to conduct phishing and spamvertising which escape notice of law-enforcement agencies and anti-cybercrime organizations. ***This is a NEVER ENDING BATTLE!***
- ❖ Internet users have to be always on alert and conduct their online transactions with care.
- ❖ Public welcome to report on phishing/spamvertising using '.hk' domains.
 - **Phone: 852 2319 1313**
 - **Email: abuse@hkdnr.hk**



H
K
I
R
C

**THANK
YOU!**



HKDNR