Report on Spamvertising and Phishing using '.hk' Domain Names and McAfee Report

ccNSO Meeting

June 24, 2008

Agenda

- ✓ Introduction of HKIRC/HKDNR and .hk Domain
- ✓ Figure of Phishing and Spamvertising
- ✓ Common Patterns of Phishing Domain
- ✓ Difficulties Encountered by Domain Registries/Registrars and How HKDNR coped with it
- ✓ McAfee Report

Introduction

- HKIRC is the registry of '.hk' ccTLD
- HKDNR is an operating arm of HKIRC in .hk domain administration.
- HKIRC/HKDNR is a registry and a registrar (combination model) for .hk domain administration
- 163,896 '.hk' domain registrations as on 1 Jun 2008
- HKDNR set up since 2001. The first phishing domain was reported in Sept 2006, as the time 2nd level of '.hk' was actively promoted into the overseas market

.hk Domain

- **Categories and Requirements of registration**

English Domain	Chinese Domain	Requirement
.com.hk	.公司.hk	Businesses / companies registered in HK
.net.hk	.網絡.hk	Entities managing network infrastructure, machines and services with a license (IVANS / ISP) from OFTA of HK
.org.hk	.組織.hk	Not-for-Profit organizations registered in HK
.edu.hk	.教育.hk	Registered schools, tertiary institutions and other approved educational institutions in HK
.gov.hk	.政府.hk	Government Bureaux / Departments of HK
.idv.hk	.個人.hk	HK Residents (for .個人.hk, domain shall be the legal name of registrant)
.hk	.hk	Local and overseas individual and entities. No documentary proof is required

Phishing and Spamvertising

(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.

- **Spamvertising** is the practice of sending E-mail spam, advertising a website. In this case, it is a portmanteau of the words “spam" and “advertising“. Spamvertisers insert links to their websites (typically, sites purporting to sell some commercial product). The links typically lead to pills, porn and poker sites.

Figure of Phishing and Spamvertising on .hk domains in 2007 & Jan 08

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
Jan 2008	*259*

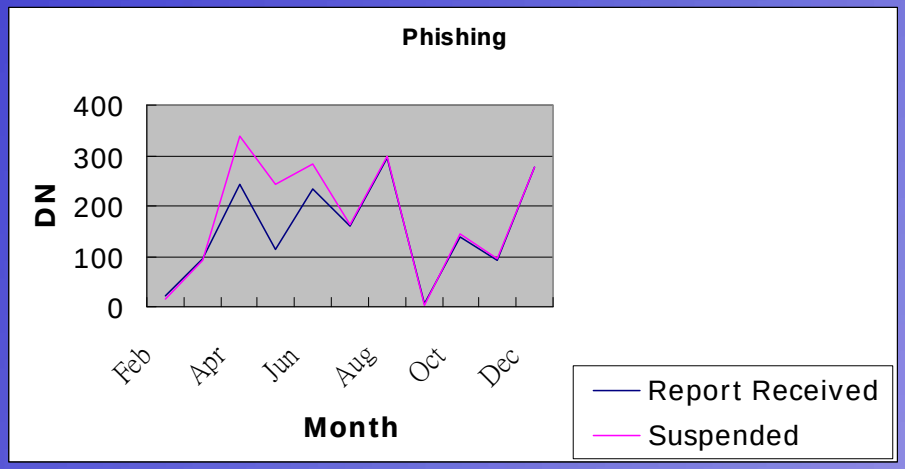
Report of Spamvertising

Month	No. of .hk domain reported for Spamvertising
Jan 2007	35
Feb 2007	66
Mar 2007	105
Apr 2007	643
May 2007	1046
Jun 2007	1326
Jul 2007	8321
Aug 2007	71
Sep 2007	20
Oct 2007	299
Nov 2007	9
Dec 2007	33
Jan 2008	10

* 1,552 spamvertising domains were found and reported by HKDNR in July 07

Figure of Phishing and Spamvertising on .hk domains (Jan 07 – Jan 08)

Graph Showing Phishing Report (Received VS Suspended)



Graph Showing Spamvertising Report (Received VS Suspended)

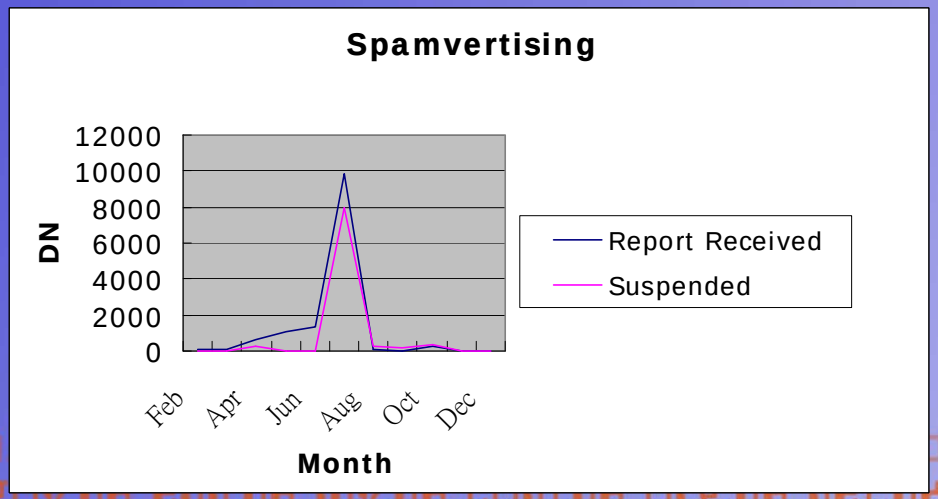


Figure of Phishing and Spamvertising on .hk domains (May 07 - May 08)

Report of Phishing

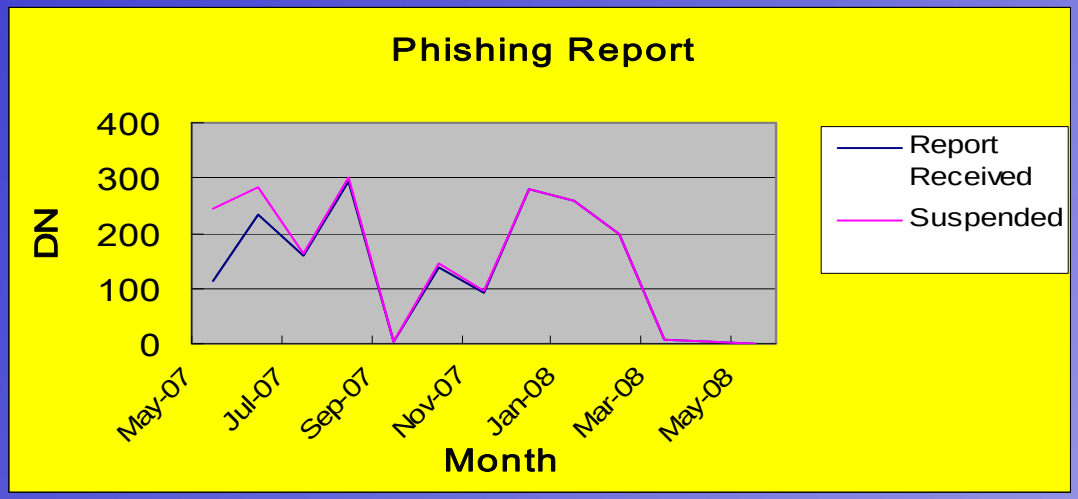
Month	No. of .hk domain reported for Phishing
May 2007	114
Jun 2007	234
Jul 2007	159
Aug 2007	294
Sep 2007	5
Oct 2007	139
Nov 2007	93
Dec 2007	278
Jan 2008	259
Feb 2008	200
Mar 2008	8
Apr 2008	3
May 2008	1

Report of Spamvertising

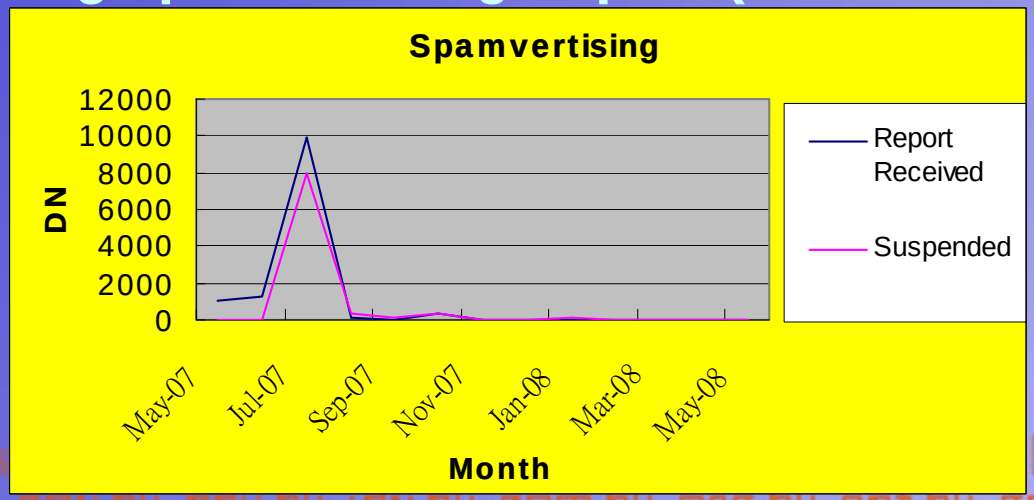
Month	No. of .hk domain reported for Spamvertising
May 2007	1046
Jun 2007	1326
Jul 2007	8321
Aug 2007	71
Sep 2007	20
Oct 2007	299
Nov 2007	9
Dec 2007	33
Jan 2008	10
Feb 2008	1
Mar 2008	12
Apr 2008	6
May 2008	1

Figure of Phishing and Spamvertising on .hk domains (May 07 – May 08)

Graph Showing Phishing Report (Received VS Suspended)



Graph Showing Spamvertising Report (Received VS Suspended)



Control Measures of Phishing and Spamvertising on .hk domains

Feb-07 and before:

-Based on the report from HKCERT, HK Police, HKDNR verified, suspended phishing domain

-Registration Agreement was amended

Mar-Apr 07:

-HKCERT helped develop guidelines to verify phishing domains so the verification process became faster

-HKDNR did verification exercise for spamvertising domains

Jun-Jul 07:

-HKDNR adopted new online payment method (restricted to accept VBV only / secure code ready credit card)

-Upon liaison by OFTA, an international blacklist provider started to provide daily spamvertising list to HKDNR; hence more than 7,000 domains were suspended in Jul

Aug 07:

-Daily monitoring of new Registration with suspicious payment and registration pattern (e.g. used lost card to settle payment, etc)

-Article posted on spamtracker.eu to fight against phishing and spamvertising domains

Sept 07:

-Article was producing effect, so the numbers decreased

Oct-Dec 07:

-Situation was back to normal

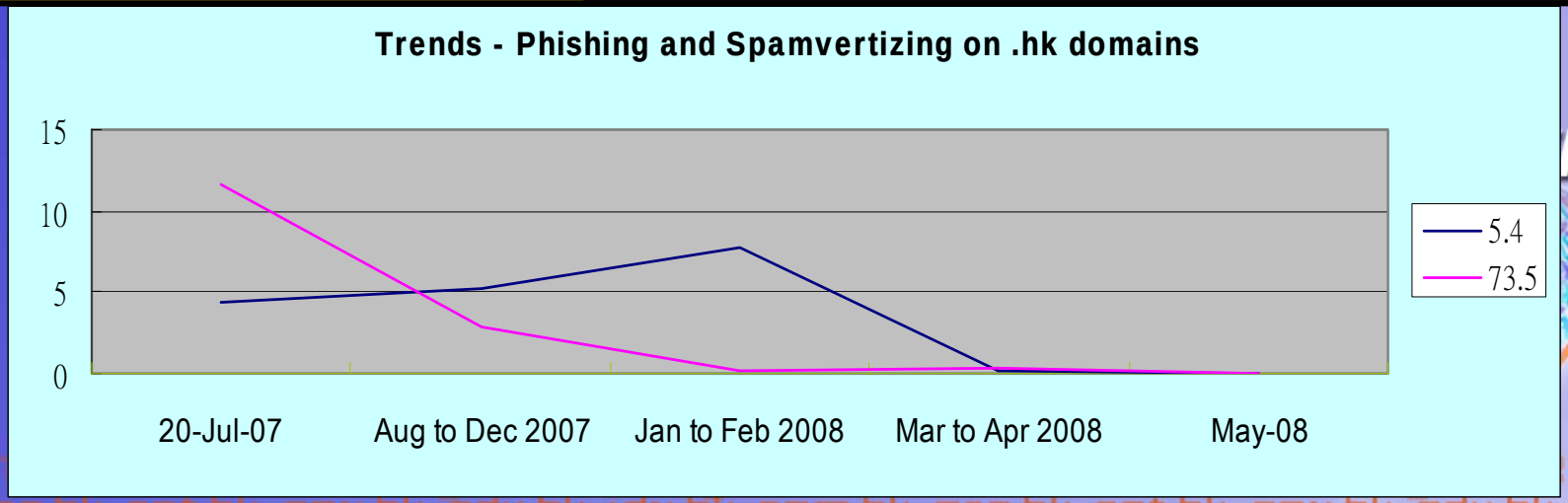
-The registrants applied more than 5 new domains at one time; so the numbers had started to increase

From Jan 08 onwards :

-HKDNR required documentary proofs for new domain name applications which are suspicious

Figure of Phishing and Spamvertising on .hk domains (Jul 07 – May 08)

	No. of .hk PHISHING domains reported per day	No. of .hk SPAMVERTISING domains reported per day
Before suspension of >7,000 domains in Jul 2007(20-Jul-07)	5.4	73.5
After suspension of >7,000 domains in Jul 2007 (20-Jul-07)	4.3	11.7
Aug to Dec 2007	5.3	2.8
Jan to Feb 2008	7.7	0.2
Mar to Apr 2008	0.2	0.3
May 2008*	0.03	0.03



What we have found so far?

- Some reported domains were used for bogus financial business website (e.g. Royal Bank of Scotland, Alliance Leicester Bank, SunTrust, Capital One Bank and eBay, HSBC etc)
- Some reported domains involved in non-financial sites like pharmacy, casino, porn website
- Many of these registrants applied 4-9 other domains at one time.
- Many reported domains were connected to name servers or addresses which follow specific patterns
- Many made payment by using several different credit cards until it succeeded
- Nearly all the reported phishing domains are 2nd level .hk domain
- Many of the phishing/spamvertising domains also identified by Firefox as suspected forgery website. Other sources: Antiphishing Group, SpamTrackers

Common Difficulties Faced by Domain Registry/Registrar and How HKDNR coped with it

Common Difficulties Faced by Domain Registries/Registrars	What have been done by HKDNR
1) Do not have expertise to verify if the reported domain is a phishing / spamvertised domain	❖ HKCERT and OFTA offered help in establishing our own verification guideline for phishing and spamvertising ❖ 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	❖ amend registration agreement so as to give more flexibility and right to take action
3) Too much domain registration barrier will be too complicated for user registrations	❖ will be flexible to set barrier for a period of time when it is at CRISIS Level

Participation in Regional / International Events

- Involvement and participation in Regional / international conferencing to make effort on combating phishing and spamvertising sites of using ccTLDs
  - **- Digital Phishnet Conference, Singapore Jan 08**
  - **- APCERT Annual Conference, Hongkong Mar 08**
  - **- Internet and DNS Security(WCSC), KL May 08**
  - **- CeCOS II Conference**
    - **(Anti-phishing Working Group) May 08**

McAfee Report

- McAfee published a report on “Mapping the Mal Web Revisited” in May 2008. The first report was published in Mar 2007.
- This report said “Hong Kong (.HK) soared in 2008 to become the most risky country TLD.” and
- “Hong Kong (.hk), which was ranked twenty-eighth most risky overall in 2007, is now the most risky TLD. ”
- In fact, the report covered a research for which most data was collected in 2007. But the report called their ranking “2008 ranking”. This mislead readers into thinking that ‘.hk’ is now very dangerous to use.

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**

HKIRC

THANK YOU!