Professional Information Security Association

Phone : (852) 8104-6800
Fax : (852) 2900-8338
Email : info@pisa.org.hk
URL : www.pisa.org.hk

June 15, 2007

Government Chief Information Officer
Commerce, Industry and Technology Bureau
15/F, Wanchai Tower
12 Harbour Road, Wan Chai
Hong Kong
(Attn: Systems Manager (H)41)
Fax: (852) 2802 4549
E-mail: domainreview@ogcio.gov.hk

Dear Sir/Madam,

1. HKIRC should be regarded as critical infrastructure. Although its commercial nature, HKSARG should take more guidance to it. We call for Government talking a more close monitoring on the Business Continuity Plan (BCP) and information security (infosec) aspects of its operation.

(a) Attack to HKIRC or flaw in operation procedure [2A1][1] can bring down the services associated with .hk. One major mission of HKIRC is to ensure the availability of service. We observed problems of .HK unavailability some years ago. We emphasize that the "profit" of the business should be partly invested in making the infrastructure more resilient.

(b) We have seen an explosion in the abuse of use of .hk in 2007. .HK domain was used to provide dynamic pointer to phishing sites, spamming servers and other fraudulent services. The use of domain name to replace IP addresses can prolong the life of these sites and hinder the enforcement of law. The only possible and effective response party if the HKDNR,yet we observed that the reports keep on rising [2B1][2]. "This is primarily attributed to a large number of .hk domains bought from a single registrar, which was slow to remove the offending domains." [2B2][3] "The CastleCops PIRT Squad observed that SEVERAL fraud categories hosted exclusively on ".hk" domains. These are the longest-lived rock phish in more than six months." [2B3][4]

The Government should put this in the priority operation objective of HKIRC/HKDNR.

1 [2A1] HK domain access problem 1 Nov 2004
http://www.legco.gov.hk/yr04-05/english/panels/itb/papers/itb1108cb1-164-1e.pdf
2 [2B1] .HK Abuse Reports
http://www.dslreports.com/nsearch?q=.hk&action=Go
3 [2B2] An Empirical Analysis of the Current State of Phishing Attack and Defence
http://www.cl.cam.ac.uk/~rnc1/weis07-phishing.pdf
4 [2B3] Crisis in Hong Kong (rock phish on .hk)
http://www.mail-archive.com/phishing@whitestar.linuxbox.org/msg00210.html

Phone : (852) 8104-6800
Fax : (852) 2900-8338
Email : info@pisa.org.hk
URL : www.pisa.org.hk

Professional Information Security Association

(c) Chinese domain name may be preyed in the next stage by fraudulent party to host phishing site again of other economies. Fraudulent parties may register "sister" domain using another language (which include Chinese) to evade the traditional detection mechanism developed for brand management service. This is the next security threat of .HK domain.

(d) The Board of Directors should consider including information security representatives or government infosec team representatives to make sure the direction be infosec sensible.

2. We support the Registry-Registrar proposal. It can help encouraging more players. The consequence is service-price improvement. It helps HKIRC focusing the service as the registry. We call to ensure the arrangement to cater the effectiveness of enforcement of fraud management as mentioned previously be developed in the registry-registrar model.

We appreciate our opinions to be considered. Should there is any inquiry, please contact us at telephone 81046800 or email: info@pisa.org.hk

Yours faithfully,

Mr. Howard Lau
Chairperson
Professional Information Security Association