HKCERT Annual Report 2010

1. About HKCERT

1.1. Establishment

- Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) was established in 2001 with funding from the Hong Kong Special Administrative Region (HKSAR) Government. The Hong Kong Productivity Council (HKPC), which is a government subvented organization in Hong Kong, has operated the centre since then.

1.2. Mission and Constituency

- HKCERT is the centre of coordination of computer security incident response for local enterprises and Internet users in Hong Kong. Her missions are to handle computer security incident reports, gather and disseminate information relating to security issues, advise on preventive measures against security threats, promote information security awareness, and maintain network with other computer emergency response teams (CERT) and security organizations to facilitate coordination and collaboration.

1.3. Organization

- The senior management of HKPC oversees the overall direction and operation of the centre. The daily operations are taken care by the Centre Manager, two consultants and a group of computer security specialists.

2. Operations and Activities

2.1. Incident Handling

- HKCERT serves as a coordination centre for information security incidents of Hong Kong. HKCERT is recognized as the national CERT for the economy of Hong Kong and the point of contact in cross border information security incidents.
- During the period from January to December of 2010, HKCERT had handled 1152 incidents, including 980 security incidents, 162 virus incidents and 11 other incidents. Security incident reports continue to overtake virus incident reports (See Figure 1).

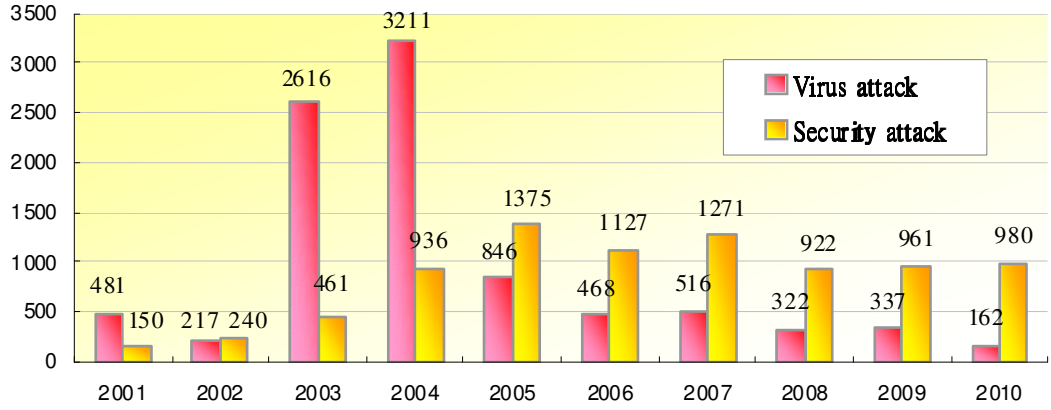

Figure 1. HKCERT Incident Reports in 2010

- The number of incidents reported by local parties was 360 (26.3%), by overseas parties was 554 (40.6%) and by proactive discovery was 452 (33.1%). The figures indicated several critical points.
  - The low local reports indicated that malware nowadays are more stealth than before. We have to do more awareness promotion to educate the general public. HKCERT has to build up a stronger malware collection and analysis capability.
  - The significant number of cross border incidents reflected the globalization of cyber attacks. A strong international collaboration is essential to success in security assurance.
  - The number of incidents we proactively discovered was more than that of locally reported incidents. We have to conduct proactively research to

effectively discover previous unreported incidents.

- For proactively discovered incident reports, we mean those incidents which are not reported by any other, but by discovery research of HKCERT staff. Our staff kept track of third party sources of malware hosting websites and command and control centres. We also monitor security researcher information sources and use the keywords of active exploit script names and related domains as keywords in search engine to locate suspicious websites. Out of all 452 proactively discovered incident reports, 33.4% were defacement websites, 31.6% were phishing sites and 14.8% were SQL injection. Code injected websites usually contained links redirecting users to exploit hosting websites. These sites have potential to cause financial loss to users. An important remark for this section is, HKCERT could not invest much resource on proactive discovery of security incidents due to commitment to other services and the current method was very manual and tedious. If we could invest more resources on automation and researches of proactive discovery, we could foresee a significant rise of discovered incidents.

2.2. Information Gathering and Dissemination

- HKCERT collected security-related information from security organizations, made judgments on the impact to Hong Kong, and decided whether to disseminate the information. During the period from January to December of 2010, **HKCERT published 308 security bulletins and advisories (See Figure 2) which is a 40% increase from previous year's number** (i.e. 220). All security bulletins were related to vulnerabilities and no malware alert was published during this period.

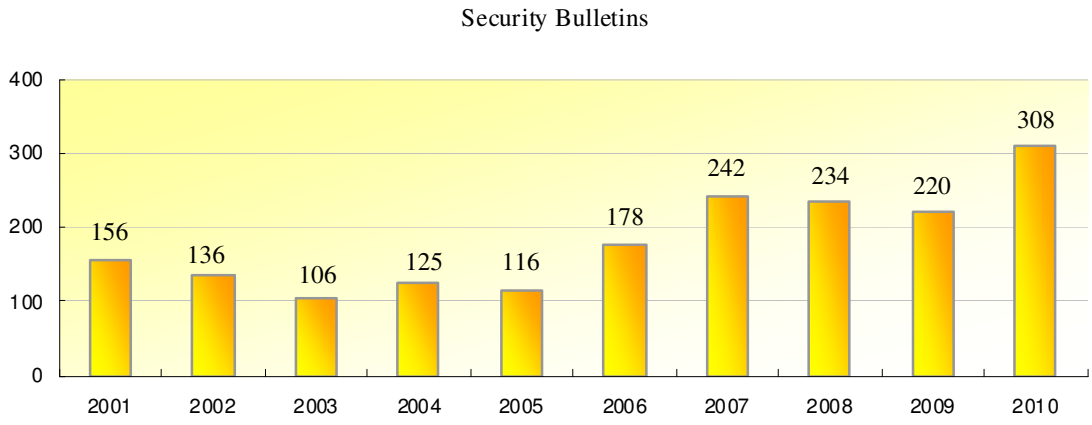

Figure 2. HKCERT Published Security Bulletins in 2010

- The major software vendors (Microsoft, Adobe and Oracle) were adopting a

practice to disclose vulnerabilities on a specific date in each month. This was a good practice for enterprise patch management. However it had also put great pressure on HKCERT's capability to disseminate the large number of security bulletins within a short period of time.

2.3. Publications

- We had published 12 issues of monthly e-Newsletter in the period.
- The **Information Express RSS feed services** continued to be well received. There were 579,809 RSS visitors in 2010, representing **a 42% increment compared with the previous year**.

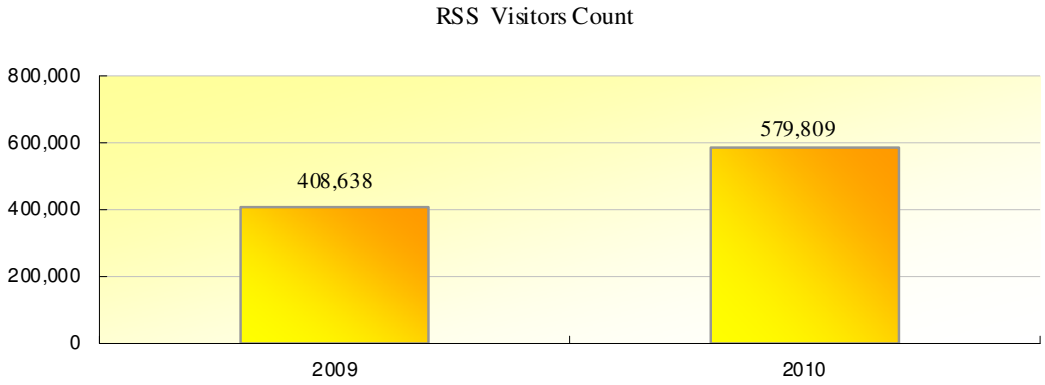

Figure 3. HKCERT RSS Visitors Count in 2010

3. Security Awareness and Training

3.1. Seminars, Conference and Meetings

- HKCERT jointly organized the Hong Kong Clean PC Day 2010 campaign with the Government and Police. The campaign involved public seminars, ISP symposium and a logo design competition. Four public seminars were organized in March May, July and November 2010.
- We organized the Information Security Summit 2010 with other organizations and associations in November 2010, inviting local and international speakers to provide insights and updates to local corporate users.

3.2. Training

- We coordinated one overseas expert and two local experts to deliver three

speeches and one hands-on workshop on “Penetration Test Kungfu with BackTrack” in the training workshops of the Information Security Summit.

3.3. Speeches and Presentations

- HKCERT was invited to deliver speeches and presentations on various occasions for Government, associations and schools.

3.4 Media briefings and responses

- HKCERT was interviewed by the media from time to time to give objective and professional views on information security topics and incidents.

4. Coordination and collaboration

4.1. International Collaboration

- Participated in the APCERT AGM and Conference in March 2010 in Thailand.
- Served as member of APCERT Steering Committee in 2010.
- Participated in the Microsoft Security Cooperation Program to share information
- Represented APCERT in the Advisory Council of DotAsia Organization
- Joined the Tsubame distributed honeypot project of JPCERT/CC
- Participated in the APCERT Drill in January 2010. HKCERT was leader of organizing committee and acted as the Exercise Control team member. The theme of the drill this year was “Fighting Cyber Crimes with Financial Incentives.” The drill was a great success with 16 teams from 14 economies participating.
- Participated in panel discussion “What’s Next for Corporate Security Incidents” in the INTERPOL Information Security Conference 2010 in Hong Kong in September 2010
- Participated in FIRST TC and CNCERT/CC Conference in September 2010 in Beijing, China and delivered a talk on APCERT Drill
- Participated in the SecureAsia@Singapore Conference of (ISC2) in July 2010 and acted as a panelist.
- Delivered speech in the Macau CERT and Manetic “Botnets, DDoS Trends and Security Countermeasures“ seminar in July 2010
- Participated in the APEC TEL41 Working Group Meeting held in Taipei in May 2010. As the chair of APCERT, HKCERT delivered two speeches on "APCERT

Drill 2010 (summary report)" and "Emerging Security Threat Landscape of the region."

- Participated in the FIRST AGM and Conference, and CERT/CC's Collaboration Meeting for CSIRT with National Responsibility in June 2010 in Miami, Florida.
- Participated in other international conferences: Digital Crime Consortium Conference in Montreal, Canada in October 2010.

4.2. Local Collaboration

- Continued to work closely with the government and law enforcement agency, and held meetings to exchange information and to organize joint events regularly
- Continued to work with police, ISPs and domain registries on closing down bulletproof hosting, phishing sites and botnet command and control centres in Hong Kong. HKCERT is still working closely with HKIRC on pre-empting the risks caused by Conficker worm generating pseudo-random domains with ".hk".
- Coorganized a local drill with HK Police and OGCIO in October 2010. Some critical information infrastructure (HKIX, HKIRC. HKISPA) and ISPs were involved. HKCERT led the preparation of the scenarios and acted as the lead of EXCON of the drill. The drill was a great success.
- Participated in the government's Information Infrastructure Liaison Group and Information Security Task Force and provided security status reporting during Internet traffic impact by Japan earthquake, and important events such as the policy address of CE and the budget speech
- Established a Information Security Advisory and Collaboration (ISAC) Mailing list and advised on latest information security issues through the list
- Organized a round table discussion meeting with information security organizations
- Liaised with Macao CERT in her application to APCERT and FIRST

5. Other Activities

5.1 Year Ender press briefing

- HKCERT planned to conduct a year ender press briefing in January 2011 to review the statistics of security incident reports and give perspective of the trend of security attacks to arouse public awareness.

5.2 Website revamp

- HKCERT was working on a new website which was planned to launch in the first quarter of 2011 to enhance the public services. The website supports mobile device and has social network feature. The security of the HKCERT website would be enhanced by adopting SSL protection for all pages. In the new website, security bulletins would be given severity rating to help users to prioritize their mitigation measures.

6. Future Plans

6.1 Funding

- HKCERT would secure Government funding to provide the basic CERT services in 2011/2012. We shall work closely with the government to plan for the future services of HKCERT.
- We shall continue to propose new initiatives to the government and seek support from the government.

6.2 Enhancement Areas

- HKCERT had conducted a strategic review of services in 2009 by JPCERT/CC. The review had pointed out areas of improvement which we shall plan on implementing the recommendations proposed in the third party rievew.
- From the incident report statistics we found that strengthening proactive discovery could probably generate good results. We suggest investing more resources to allow tracking of more information sources and automation the process. Furthermore, malware analysis capabilities and public awareness education could directly address the threat of new malware.
- HKCERT should carry on the good local and international collaboration. A lot of global cooperation is required in incident response and we depended on Internet infrastructure players as our strategic partners to speed up the take downs. We shall continue to work closely with local ISPs and Domain Name Registries.

-- THE END --