HKCERT

Annual Report 2009

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

- During the period from January to December of 2009, HKCERT had handled 1304 incidents, including 337 virus incidents, 961 security incidents and 6 other incidents. Security incident reports continue to overtake virus incident reports (See Figure 1). In addition, the number of incidents identified through proactive discovery has also increased.

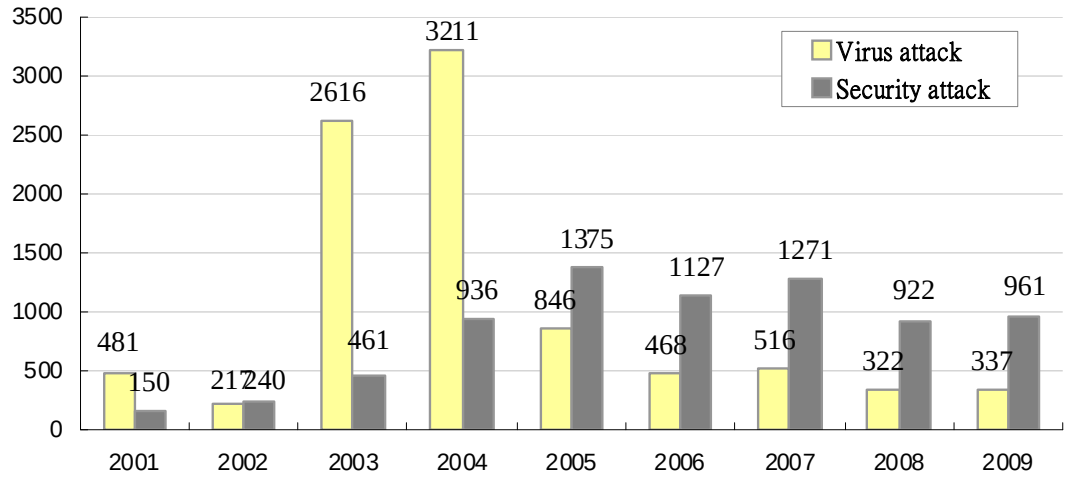

Figure 1. HKCERT Incident Reports in 2009

2.2. Information Gathering and Dissemination

- During the period from January to December of 2009, HKCERT published 220 security vulnerability alerts and advisories. No malware alert was published during this period.

2.3. Publications

- We had published 12 issues of e-Newsletter and sent out alert summaries twice per month.

3. Security Awareness and Training

3.1. Seminars, Conference and Meetings

- HKCERT jointly organized the Hong Kong Clean PC Day 2009 campaign with the Government and Police. The campaign involved public seminars, ISP symposium and an online story writing competition.
- We organized the Information Security Summit 2009 with other organizations and associations in November 2009, inviting local and international speakers to provide insights and updates to local corporate users.

3.2. Training

- We have assisted the organization of the technical training workshops of the Information Security Summit and coordinated two overseas experts to deliver hands-on workshops on “Monitoring and Analyzing Web Client Side Attacks”.

3.3. Speeches and Presentations

- HKCERT was invited to deliver speeches and presentations on various occasions for Government, associations and schools. We were also 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 Microsoft Security Cooperation Program to share information
- Represented APCERT in the Advisory Council of DotAsia.
- Joined the Tsubame distributed honeypot project of JPCERT/CC.
- Participated in the APCERT AGM and Conference and elected as the chair of APCERT.
- Participated in the APEC TEL Working Group meeting held in Singapore and delivered a speech, as the chair of APCERT, on Conficker Worm.
- Participated in the FIRST AGM and Conference and the Collaboration Meeting for CSIRT with National Responsibility organized by CERT/CC.
- Participated in the APCERT Drill on 28 January 2010 -- HKCERT took leadership in scenario preparation and acted as the EXCON. The drill was a great success.

4.2. Local Collaboration

- Provided cyber security assurance services to the East Asian Game held in Hong Kong in December 2009.
- Coordinated meetings pertaining to the Conficker worm
- 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

- Organized a local drill on 16 July 2009 and got some critical information infrastructure and ISPs involved. HKCERT prepared the scenarios and acted as the EXCON of the drill. The drill was a great success.
- Participated in the government's Information Infrastructure Liaison Group and Information Security Task Force
- Met with the Macao CERT in her startup stage to foster closer collaboration and exchange of information.

5. Other Activities

5.1. Third party service review

- HKCERT had carried out a third party review on the operations and services in November 2009 as requested by the government. JPCERT/CC was invited as the reviewer. The review covered the core operations and services, publication, organizational relationships, supporting organization, information management and human resources. Recommendations were made on the enhancing the services and coping with the future trends.

-- END --