HKCERT Annual Report 2012

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.

The mission of HKCERT is to be the Cyber Threats Response and Defense Coordinator in Hong Kong to protect the internet environment and the economic and social interests of Hong Kong.

The objectives of HKCERT are to serve as a focal point in Hong Kong for computer security incident reporting and responses; to provide a focal point in Hong Kong for cooperation and coordination with other Computer Emergency Response Teams, and relevant bodies outside Hong Kong; to promote awareness of the community on computer security issues and the latest international best practices and standards; and to provide assistance to the community in the protection against computer security threats and the prevention of security attacks and in recovery actions for computer security incidents

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, three consultants and a group of computer security specialists.

2. Operations and Activities

2.1 Incident Handling

During the period from January to December of 2012, HKCERT had handled 1,189 incidents, including 1,050 security incidents and 108 virus incidents. Security incident reports continue to overtake virus incident reports (See Figure 1).

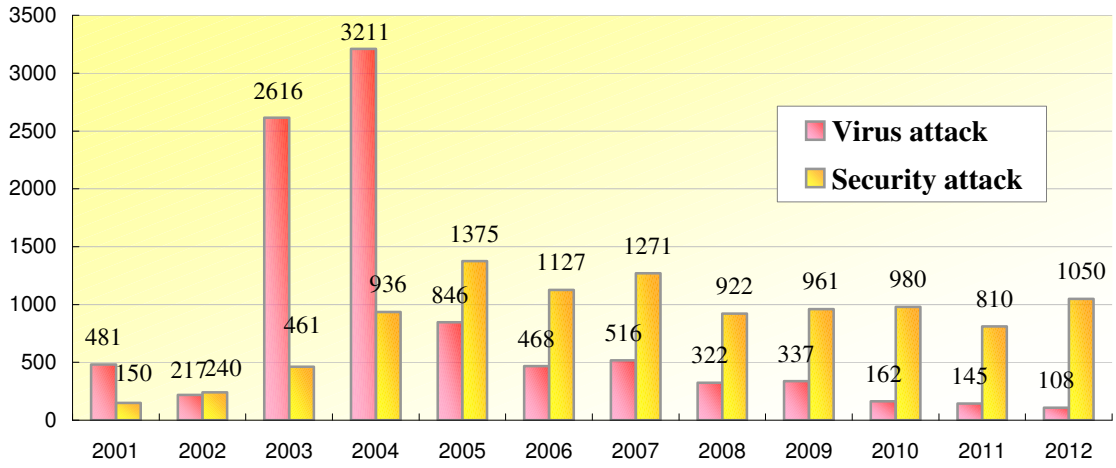

Figure 1. HKCERT Incident Reports in 2012

The total number of incidents handled by HKCERT in 2012 has increased by 22%, compared to 2011. This is mainly caused by the increase in the proactive discovery cases, in particular web defacement cases. The increase in proactive discovery cases may be caused by our improvement in the discovery process and additional resources put into proactive discovery. It also reflected the seriousness and resilience of modern malware infection and active intrusion, and the inadequacy of organizations in securing their systems.

We started to accept incident reports relating to smartphone in April 2012. During this period, we have received 18 reports in this area and most of them were relating to phishing messages.

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 2012, HKCERT

published 429 security bulletins (See Figure 2) which is a 25.1% increase from previous year's number. All security bulletins were related to vulnerabilities and no malware alert was published during this period. In addition, we have also published 58 blogs and advisories, including security advice on the use of smartphone and the best security reads of the week.

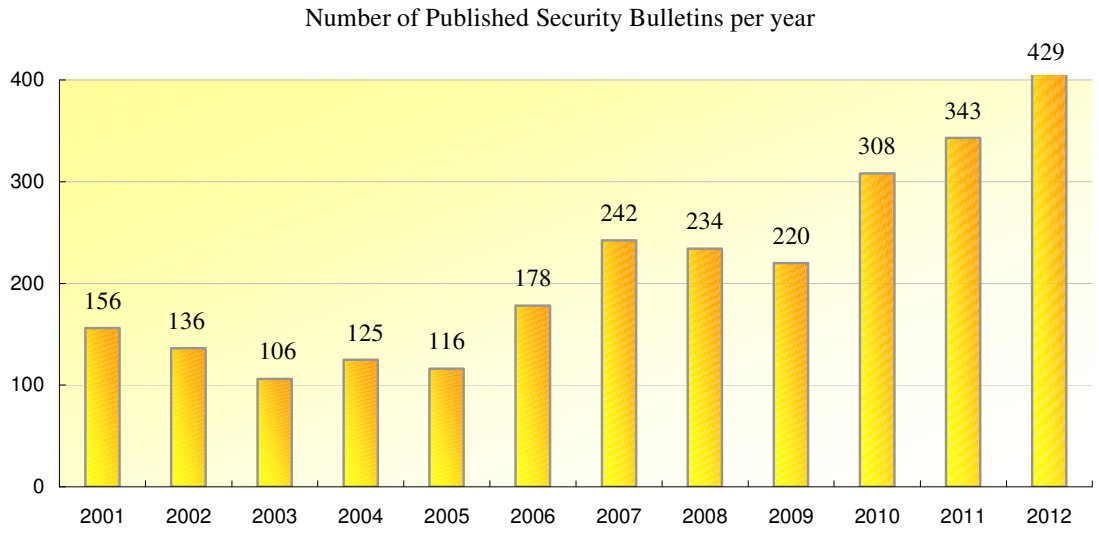

Figure 2. HKCERT Published Security Bulletins in 2012

2.3 Publications

We had published 12 issues of monthly e-Newsletter in the period.

3. Security Awareness and Training

3.1 Seminars, Conference and Meetings

HKCERT jointly organized the "Build A Secure Cyberspace" campaign with the Government and HK Police. The campaign involved public seminars, a cyber security symposium for ISPs, and a poster design contest. Four public seminars were organized in March, May, August and December 2012.

We organized the Information Security Summit 2012 with other information security organizations and associations in November 2012, inviting local and international speakers to provide insights and updates to local corporate users.

3.2 Speeches and Presentations

HKCERT was invited to deliver speeches and presentations on various occasions

for the Government, associations and schools.

3.3 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

HKCERT participated in a number of international coordination and collaboration events:

- Participated in the APCERT AGM and Conference in Bali, Indonesia; the FIRST AGM and Conference in Malta; and the Annual Meeting for CSIRTs with National Responsibility in Malta.
- Participated in the APCERT Drill (February 2012) and acted as the Exercise Control team member. The theme of the drill this year was "Advance Persistent Threats and Global Coordination". The drill was a great success with 22 APCERT teams from 17 economies participating.
- Participated in International honeypot initiatives, including joining the Tsubame project of JPCERT/CC and the Honeynet Project.
- Represented APCERT in the Advisory Council of DotAsia Organization

4.2 Local Collaboration

HKCERT worked with a number of local organizations in different areas:

- 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". In 2012, HKCERT had worked with ISPs to clean up DNS Changer infected machines in Hong Kong.
- Co-organized a local drill with HK Police and OGCIO on 31st October 2012 with players from ISPs and Domain Name registrars in Hong Kong. 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 the Cloud Security and Privacy Working Group.
- Maintained the Information Security Advisory and Collaboration (ISAC) Mailing list with the Internet Infrastructure organizations, and advised on latest information security issues through the list
- Organized an industry networking session with information security organizations in Hong Kong.

5. Other Activities

5.1 Year Ender press briefing

HKCERT organizes a year ender press briefing to media at the beginning of each year, to report on information security status in the past year, and to give perspective of the trends of security attacks in the coming year to warn the public for better awareness and preparedness. The 2012 year ender briefing was held on 5th January 2012 to talk on the security status of 2011 and trends of 2012.

5.2 Three Year Strategic Plan

HKCERT prepared its first Three Year Strategic Plan and presented to the government. The plan will be updated annually.

6. Future Plans

6.1 Funding

HKCERT would secure Government funding to provide the basic CERT services in 2013/2014. 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 is working on adding critical security bulletins messages to the GovHK Notifications mobile application (a one-stop platform for citizens to receive Hong Kong Government notifications.)
- HKCERT is working on an Information Feed Analysis System to collect intelligence of compromised machines in Hong Kong. The system will

provide a better picture of security status of Hong Kong and help clean up the botnets and C&C servers in Hong Kong.

- HKCERT is also developing a new Incident Report Management System which will help improve the efficiency of our incident response activities.
- HKCERT is enhancing the liaison and information sharing with the critical infrastructure sector to better protect the security environment of Hong Kong.

-- END --