# HKCERT Annual Report 2011

## 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 2011, HKCERT had handled 975 incidents, including 810 security incidents, 145 virus incidents and 20 other incidents. Security incident reports continue to overtake virus incident reports (See Figure 1).

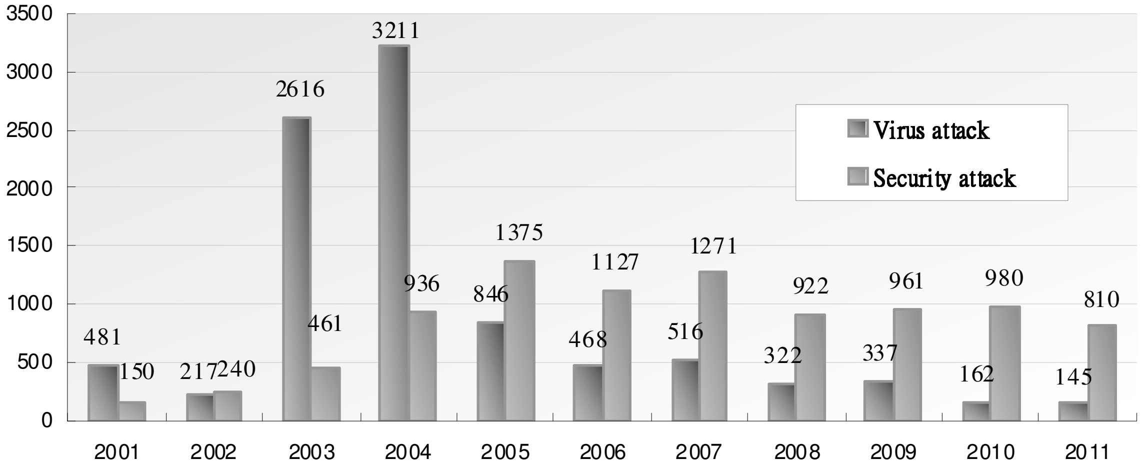

*Figure 1. HKCERT Incident Reports in 2011*

The number of incidents reported by local parties was 400 (34.3%), by overseas parties was 405 (34.7%) and by proactive discovery was 360 (30.9%).

| **Source locality of reports** | **2010** | **2011** |
|---|---|---|
| Local parties | 360 (26.3%) | 400 (34.3%) |
| Overseas parties | 554 (40.6%) | 405 (34.7%) |
| Proactive discovery | 452 (33.1%) | 360 (30.9%) |

- The continuing low local reports indicated that malware nowadays are more stealth than before. We have to do more awareness promotion to educate the general public about the threats.
- The significant number of cross border incidents reflected the globalization of cyber attacks and a need for building strong international collaboration.
- We have to conduct proactively research to effectively discover previous unreported incidents.

Proactively discovered incident reports are a result of discovery research conducted by HKCERT staff. Defacement websites and phishing sites were among the top 3 in 2010 and 2011. In 2011, malware infection climbed up to second and code injection (9.2%) went to the fourth place,

| Top 3 incident types via Proactive Discovery | 2010 | 2011 |
|---|---|---|
| 1 | Defacement (33.4%) | Defacement (33.9%) |
| 2 | Phishing (31.6%) | Malware (25.8%) |
| 3 | Code Injection (14.8%) | Phishing (23.9.9%) |

## 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 2011, HKCERT published 343 security bulletins and advisories (See Figure 2) which is an 11% increase from previous year's number (i.e. 308). All security bulletins were related to vulnerabilities and no malware alert was published during this period.

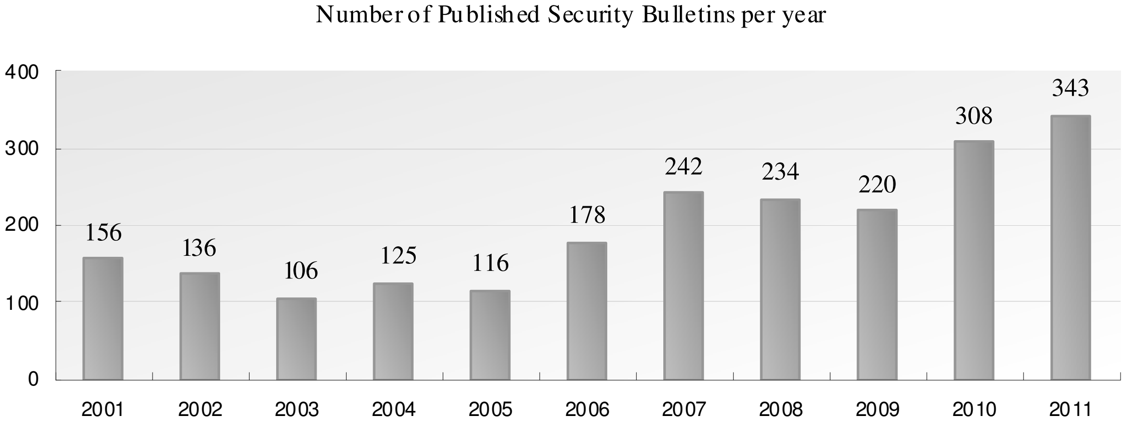

*Figure 2. HKCERT Published Security Bulletins in 2011*

## 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 1,182,911 RSS visitors in 2011, representing **a 104% increment compared with the previous year.**

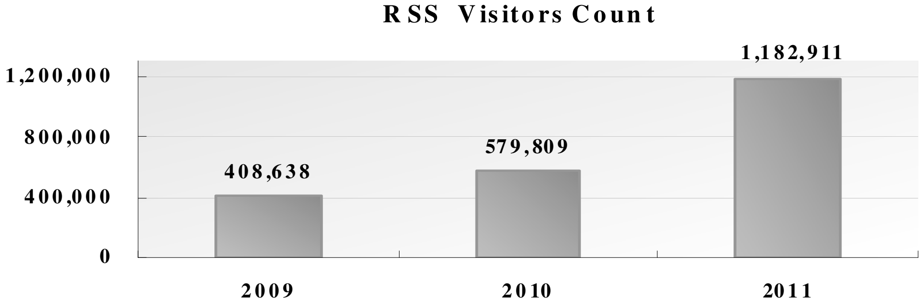

*Figure 3. HKCERT RSS Visitors Count in 2011*

## 3. Security Awareness and Training

### 3.1 Seminars, Conference and Meetings

HKCERT jointly organized the Hong Kong Clean PC Day 2011 campaign with the Government and Police. The campaign involved public seminars, cyber security symposium and a screensaver contest. Five public seminars were organized in March, June, August, October and December 2011.

We organized the Information Security Summit 2011 with other organizations and associations in November 2011, inviting local and international speakers to provide insights and updates to local corporate users.

### 3.2 Training

We coordinated two overseas expert and two local experts to deliver three speeches and three hands-on workshop on “Analysis and Reverse Engineering Android Malware”, “Deploying a Secure Private Cloud” and “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

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

4.1.1 Collaboration with CERT community

- Served in the APCERT Steering Committee in 2010-2012; elected as the Chair for 2010-2011
- Participated in APCERT AGM and Conference 2011 in Jeju, Korea (March 2011)
- Participated in both the FIRST AGM and Conference 2011, organized by FIRST, and the Annual Meeting for CSIRTs with National Responsibility, organized by CERT/CC in Vienna, Austria (June 2011)
- Participated in the APCERT Drill (Feb 2011) and also acted was the Exercise Control team member. The theme of the drill this year was "Critical Infrastructure Protection". The drill was a great success with 20 APCERT from 17 economies participating.
- Joined the Tsubame distributed honeypot project of JPCERT/CC
- Liaised with Macao CERT (MOCERT) in her application to APCERT and FIRST and paid a site visit to MOCERT (May 2011)

4.1.2 Collaboration with other international organizations

- Represented APCERT in the Advisory Council of DotAsia Organization
- Joined the Microsoft Security Cooperation Program to share information
- Participated in Digital Crime Consortium Conference in the Bahama Islands, organized by Microsoft (Oct 2011)
- Participated in Honeynet Project Workshop 2011 in Paris (March 2011)
- Participated in the AVAR Conference in Hong Kong (Nov 2011)

### 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".
- Co-organized a local drill with HK Police and OGCIO on 4th November 2011 on web forum incident response. 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 World IPv6 Day, and important events such as the policy address of CE and the budget speech
- Maintained the 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

## 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 2011 year ender briefing was held on 4th January 2012.

### 5.2 Website revamp

HKCERT revamped the website and launched it officially in 2011. The website supports mobile device and has social network feature. The security of the HKCERT website was 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 2012/2013. 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 by JPCERT/CC in late 2009. The review had pointed out areas for improvement which we are working on thean strategic plan to incorporate implementation plan on these recommendations in future plan and seek funding to support them.. They include enhancement of incident management system, proactive discovery of security incidents, intelligence collection,

From the incident report statistics we found that strengthening proactive discovery could probably generate good results. We plan to invest more resources to allow tracking of more information sources and automation the process. mobile security incident handling and malware analysis capability.

**-- END --**