# HKCERT Annual Report 2014

## 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 Organization and Workforce power

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 six Security Analysts and one Administrative Assistant.

### 1.3 Mission and Constituency

HKCERT is the centre of coordination of computer security incident response for the constituency (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 information security incident reporting and responses; to provide a focal point in Hong Kong for cooperation and coordination with other Computer Emergency Response Teams (CERTs), 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

## 2. Activities and Operations

### 2.1 Incident Handling

During the period from January to December of 2014, HKCERT had handled 3,443 security incidents which was 103% increase of the previous year (see Figure 1).

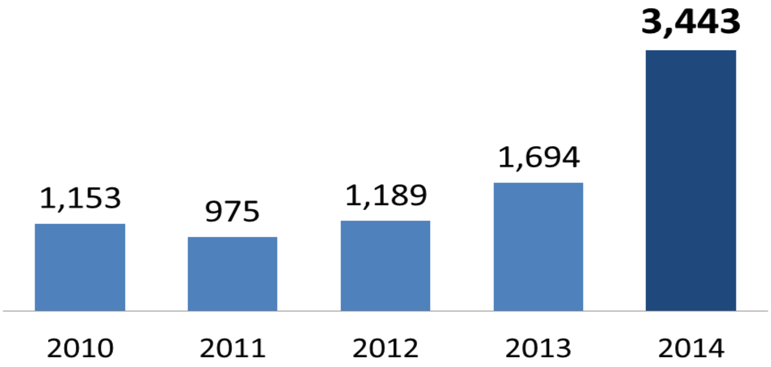

*Figure 1. Incident Reports Handled by HKCERT*

The huge increase of the number of incidents was due to the increase of referral cases as a result of closer collaboration with global security researchers and organizations. Referral cases accounted for 80% of the total number of security incidents.

The major category of security incidents was botnet (1,973 cases) which recorded a 357% increase. Next was phishing (594 cases) which recorded a 55% increase (see Figure 2).

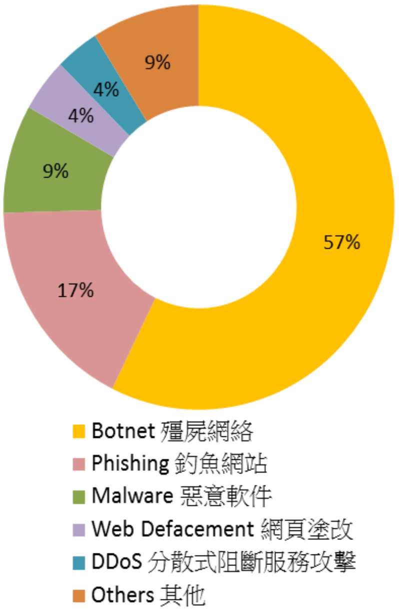

*Figure 2. Distribution of Incident Reports in 2014*

In the past few years, HKCERT had joined the global botnet takedown operations to fight cross border cyber attacks. During the period, HKCERT has participated in several global botnet take down operations against Citadel, Brobot, ZeroAccess, Zeus, GameoverZeus and Pushdo. The availability of data from overseas organizations like CERTs, security researchers, vendors and the HKCERT's automation and process streamlining allowed the handling of large amount of incidents. The number of botnet incident reports rose sharply in the past three years (see Figure 3). This increase indicated a progress of security status of Hong Kong to dig out and clean up previously "invisible" incidents.

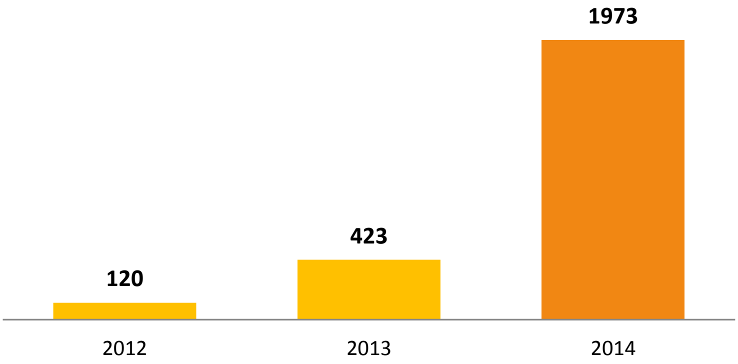

*Figure 3. Number of Botnet Incident Reports in the past 3 years*

### 2.1.1 Territory-wide Attack in October 2014

In October 2014, an international hacker group "Anonymous" declared a campaign called Operation Hong Kong (OpHongKong) against Hong Kong websites. It was the most extensive and longest territory-wide cyber attack in the history of Hong Kong, targeting websites of government departments, critical organizations, political organizations, press & media, and some other non-government organizations.

The attackers announced their target websites on social media websites and they openly recruited volunteers to join the attack. They even provide one-click DDoS (distributed denial-of-service) attack tools so that people without technical know-how could participate.

There were mainly 3 types of attacks in the campaign: web defacement, DDoS attack and intrusion of information systems respectively. For DDoS attack, attackers used web application attacks, malformed network protocols, SYN flood, volumetric attacks and Wordpress pingback as the means.

HKCERT worked closely with government information security team and the police to tackle this large scale attacks.

- informing the public of the attacks immediately and advised them how to secure their systems; warning Internet users not to participate in any cyber attacks
- monitored the target sites and exchanging information with government
- handling the incidents of non-government organizations
- informing the targets and advised them the recover actions; informed the hosting companies of the targets to be prepared for the attacks affecting their network
- issuing takedown requests to administrators of servers hosting DDoS attack scripts
- sharing the lesson learnt to the public

According to HKCERT's statistics[1], from 2nd to 22nd October 2014 there were 38 non-government websites defaced and 23 non-government websites attacked by DDoS. All of them had resumed to normal operation on 22nd October, 2014.

## 2.2 Watch and Warning

During the period from January to December of 2014, HKCERT published 348 security bulletins (see Figure 4) on the website. In addition, HKCERT have also published 126 blogs, including security advisories on WinXP end-of-support, ransomware, Heartbleed vulnerability, Shellshock vulnerability, botnet attacks, point of sales malware and DDoS and web attacks of Operation Hong Kong campaign. HKCERT also published the best security reads of the week every week to inform the public of good security articles.

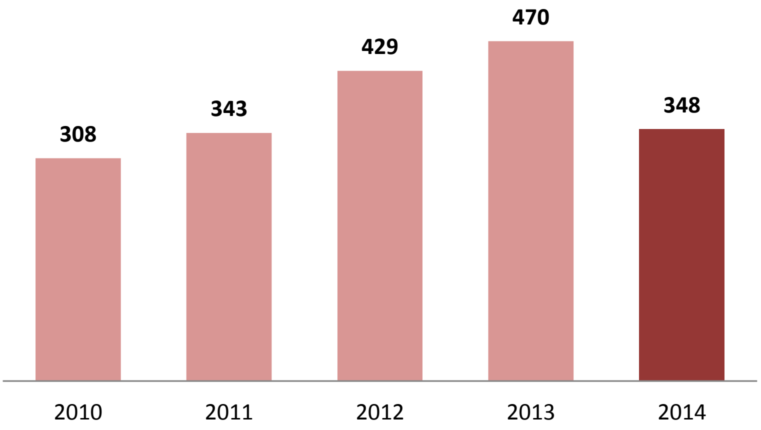

*Figure 4. HKCERT Published Security Bulletins*

[1] Information Security Status Report -- Attacks Targeting Hong Kong (2014-10-22) https://www.hkcert.org/my_url/en/blog/14102201

HKCERT used the centre website (www.hkcert.org), RSS, HKCERT mobile app, and Hong Kong Government Notification mobile app to publish security bulletins, blogs and news. HKCERT also used email and SMS to publish selected security bulletins to subscribers. The subscriptions are free of charge.

### 2.2.1 Embrace global cyber threat intelligence

HKCERT had implemented the Information Feed Analysis System (IFAS) to collect intelligence of compromised machines in Hong Kong from global security researchers. The system provided a better picture of security status of Hong Kong and can check the effectiveness of the security operations. For example, Figure 5 showed the trend of bot related security events decreasing from 9,958 in Q4 2013 to 6,172 in Q4 2014. It reflected the effectiveness of the botnet takedown operation in 2014.

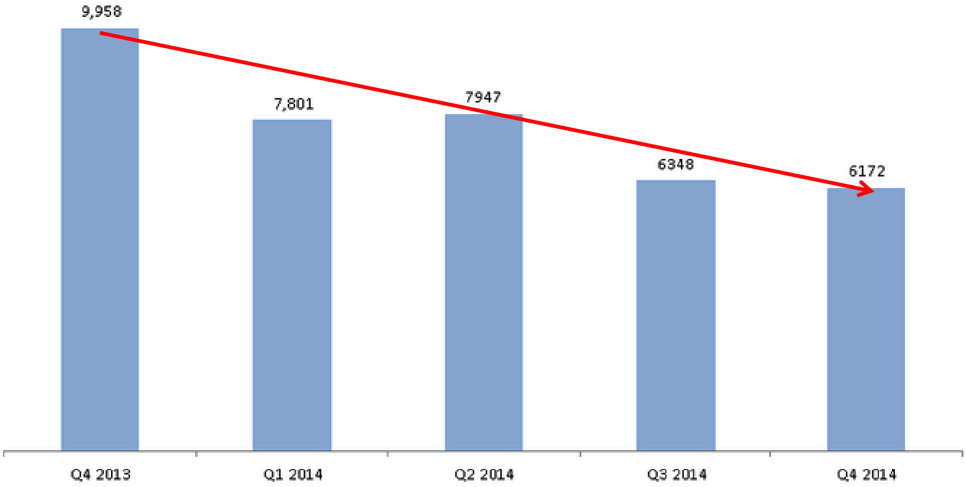

*Figure 5. Trend of Bot related security events in the past year*

*(Source: data feeds from overseas security researchers, not from incident reports)*

## 2.3 Publications

- HKCERT had published 4 quarterly issues of Hong Kong Security Watch Report showing the status of compromised computers in Hong Kong from the data collected from overseas security researchers (see https://www.hkcert.org/hkswr).

- HKCERT had published 12 issues of Hong Kong Google Play Store's Apps Security Risk Report. The Report is a co-operation with CNCERT/CC of China (see https://www.hkcert.org/play-store-srr).

香港地區 Google Play 商店
應用程式保安風險報告
CNCERT/CC
国家互联网应急中心
HKCERT
Hong Kong Google Play Store's Apps Security Risk Report

- HKCERT had published 12 issues of monthly e-Newsletter in the period (see https://www.hkcert.org/newsletters).

- HKCERT had published the statistics of incident reports and security bulletins every quarter (see https://www.hkcert.org/statistics).

## 3. Events organized and co-organized

### 3.1 Seminars, Conference and Meetings

HKCERT jointly organized the “Build A Secure Cyberspace” campaign with the Government and Hong Kong Police Force. The campaign involved public seminars, a cyber security symposium for ISPs, and a 4-Panel Comic Drawing contest. Four public seminars were organized in February, April, August and November 2014.

We organized the Information Security Summit 2014 with other information security organizations and associations in October 2014, 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 promotion, briefings and responses

- HKCERT published two advertorials in November 2014 to promote the public seminar and the comic drawing contest.
- HKCERT published weekly column articles in Hong Kong Economic Times starting June 2014 to give information of current information security trends and advices.
- HKCERT was interviewed by the media from time to time to give objective and professional views on information security topics and incidents.

# 4. Collaboration

## 4.1 International Collaboration

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

- Participated in the APCERT AGM and Conference in Taipei and delivered talk on IFAS
- Participated in the FIRST AGM and Conference in Boston and jointly with CERT Austria delivered talk on cyber threat intelligence collection and analysis systems; participated in the Annual Meeting for CSIRTs with National Responsibility in Boston and shared in the panel discussion the future of CERTs.
- Participated in the APCERT Drill (February 2014) and acted as member of the Organizing Committee and the Exercise Control team. The theme of the drill this year was “Countering Cyber-ops with Regional Coordination”. The drill was a great success with 20 APCERT teams from 16 economies, and 3 economies of OIC-CERT participating.
- Participated in International honeypot initiatives, including joining the Tsubame project of JPCERT/CC and The Honeynet Project.
- Participated in the Digital Crime Consortium Conference in Singapore
- Represented APCERT in the Advisory Council of DotAsia Organization

HKCERT promotes to other CERTs to use the IFAS system (the IFAS.io initiative) developed by HKCERT. The IFAS.io initiative got some pilot users. These pilot users also contributed to IFAS by providing feedback to the system. One CERT pilot user even produced a patch for the installation script.

## 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 2014, HKCERT had worked with ISPs to clean up Citadel, Brobot, ZeroAccess GameoverZeus and Pushdo botnet machines in Hong Kong.

- Co-organized a local drill with HK Police and the Office of Government Chief Information Officer (OGCIO) on 31st October 2014 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
- Liaised with critical infrastructure sector and had delivered awareness briefings to these organizations for better protecting the security environment of Hong Kong; created the Information Security Advisory and Collaboration (ISAC-CI) Mailing list with the critical infrastructure organizations, and advised on latest information security issues through the list;

## 5. Other Achievements

### 5.1 Strategy and Service Review

HKCERT had conducted a Strategy and Service Review (undertaken by AusCERT) in October 2013. The report was received by HKCERT and the Hong Kong SAR Government in March 2014.

### 5.2 CERT Study Tour

HKCERT, jointly with the OGCIO, had visited CERTs and other information security organizations in Australia, China and Japan in June and July of 2014. The mission of this tour was to broaden the horizon on contemporary CERT development and to exchange on the vision of the future of CERTs, so as to help reviewing the strategies of HKCERT. The collaboration opportunities were also sought during the visits. The visits allowed HKCERT to open the eyes and collected extremely useful information and sparked insights for the future development of HKCERT

### 5.3 Advisory Group Meeting

HKCERT had held the Advisory Meeting in Hong Kong and met with overseas advisors in international meeting venues to solicit inputs from the advisors on the development strategy of HKCERT.

### 5.4 Three Year Strategic Plan

HKCERT prepared its third rolling Three Year Strategic Plan based on inputs from Advisory Group, the Strategy and Service Review Report and the CERT Study Tour and discuss with the government. The plan would be updated annually. HKCERT based on this plan to prepare the annual plan and budget to solicit funding support from the government.

### 5.5 Embrace global intelligence and build security health metrics

HKCERT had implemented the IFAS to collect intelligence of compromised machines in Hong Kong. The system provided a better picture of security status of Hong Kong and help clean up the botnets and C&C servers in Hong Kong. HKCERT publicized the information to the public quarterly and used the information in decision making.

HKCERT also joined the Cyber Green project initiated by JPCERT/CC in an attempt to collaborate with other CERTs to build useful metrics for measuring cyber health.

## 5.6 Year Ender press briefing

HKCERT organized a year ender press briefing to media in January 2015 to report on information security status of 2014, and to give perspective of the trends of security attacks in the coming year to warn the public for better awareness and preparedness. It received very good press coverage.

*Figure 6. Mr Wilson Wong, General Manager (IT Industry Development) of HKPC (left), and Mr Leung Siu-Cheong, Senior Consultant of HKCERT of HKPC, review the information security situation in Hong Kong in 2014, and introduce the upcoming trends in the press briefing.*

## 6. Future Plans

### 6.1 Strategy

“Proactivity”, “Share to Win” and “Security is not an Island” are three directions of HKCERT. HKCERT will work closer with CERTs, security researchers and Internet stakeholders to build a more secure Hong Kong and Internet.

### 6.2 Funding

HKCERT would secure Government funding to provide the basic CERT services in 2015/2016. 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.

### 6.3 Enhancement Areas

HKCERT is working on enhancing the intranet to increase the efficiency of information search and sharing. HKCERT is also developing automation modules to enhance the use of data in the IFAS to select prioritized incidents and collect intelligence about compromised machines in Hong Kong to follow up.

## 7. Conclusion

Year 2014 was a year with big challenges in information security for Hong Kong. Hong Kong had encountered the biggest and longest territory wide attack campaign. HKCERT collaborated with the information security team of OGCIO and the Cyber Security and Technology Crime Bureau (CSTCB) of the Hong Kong Police closely to respond to the attack. This collaborated response mechanism proved to be working in the real life challenge and the communication protocol was further streamlined. The attack had also raised the public awareness on one-click DDoS. More awareness education would be required to follow up.

In 2014, HKCERT was also active in global botnet takedown operations and the cyber threat intelligence development. The cross border collaboration and intelligence driven response had improved the proactiveness and effectiveness of incident response. HKCERT also champion the sharing of IFAS with overseas CERTs. HKCERT has seen the immense power of collaboration and would invest more to further this success.

In 2014, HKCERT had set up the communication platform with some critical infrastructure organizations. To this end, we will continue to adopt collaborative approach to share information, conduct joint research and development, and develop closer relationship with our partners.

With the Internet security facing more crises from cyber conflicts, ransomware, POS attacks, exposure of Internet devices and new security challenges arising from adoption of emerging technologies like cloud computing, mobile payment and Internet of things, HKCERT would expect a more challenging year 2015.

**-- END --**