HKCERT Annual Report 2015

Hong Kong Computer Emergency Response Team Coordination Centre,

Hong Kong Productivity Council

HKCERT Annual Report 2015

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 2015, HKCERT had handled 4,928 security incidents which was 43% increase of the previous year (see Figure 1).

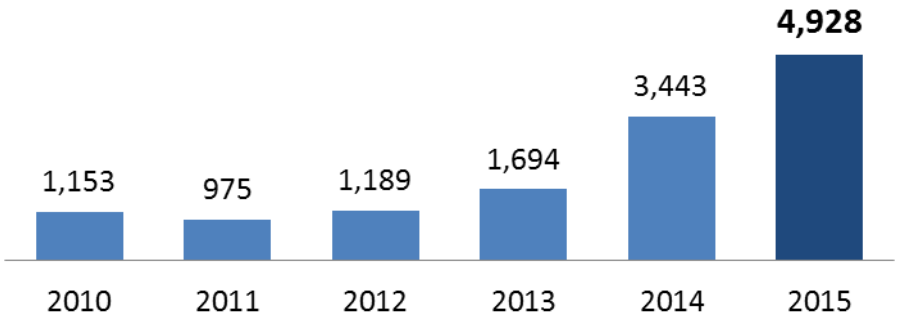

Figure 1. Incident Reports Handled by HKCERT

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 phishing (1,978 cases) which recorded a 233% increase. Next was botnet (1,943 cases) (see Figure 2).

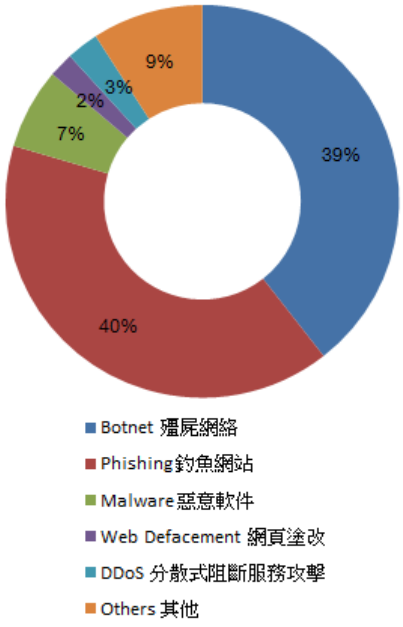

Figure 2. Distribution of Incident Reports in 2015

In the past few years, HKCERT keeps working on the phishing website taken down operations to protect the Internet users from phishing fraud. In 2015, the number of phishing incident reports rose sharply by 233% (see Figure 3). These phishing websites were running as new “flash” phishing attacks that were launched using local web hosting services as cover.

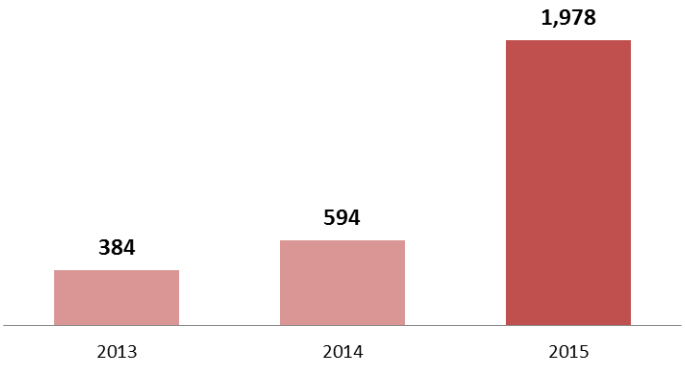

Figure 3. Number of Phishing Incident Reports in the past 3 years

2.2 Watch and Warning

During the period from January to December of 2015, HKCERT published 352 security bulletins (see Figure 4) on the website. In addition, HKCERT have also published 111 blogs, including security advisories on Windows Server 2003 end-of-support, fraudulent email, phishing scam, ransomware, mobile malware, vulnerabilities on Internet devices, and botnet attacks. HKCERT also published the best security reads of the week every week to inform the public of good security articles.

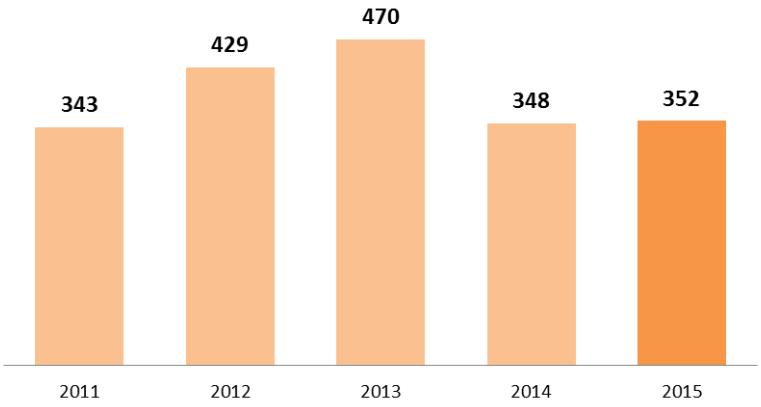

Figure 4. HKCERT Published Security Bulletins

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 slightly decreasing from 6,172 in Q4 2014 to below 6,000 in 2015. Figure 6 showed the trend of top 5 botnet families in the past year. Besides a new botnet family Bamital raised in Q2 2015, the overall decreasing trend of other botnet families reflected the effectiveness of the botnet takedown operation.

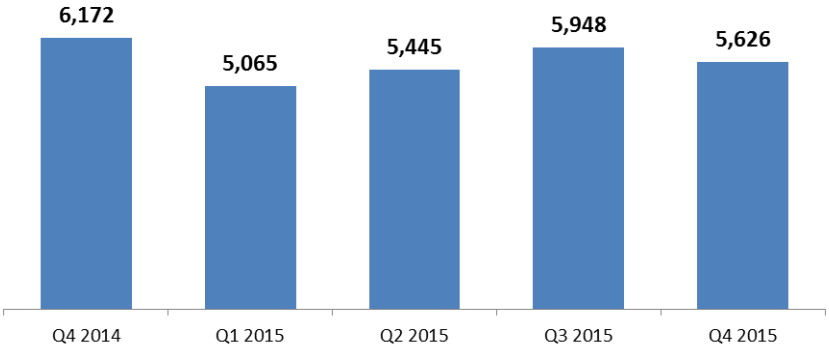

Figure 5. Trend of Bot related security events in the past year

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

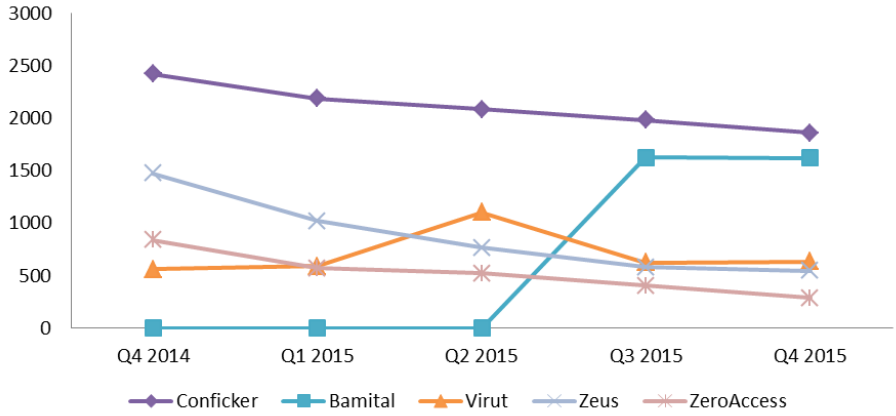

Figure 6. Trend of Top 5 Botnet Families in the past year

(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).

- 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 “Cyber Security is Everywhere” campaign with the Government and Hong Kong Police Force. The campaign involved public seminars, and a graphic design contest. Two public seminars were organized in April and November 2015.

For the graphic design contest, HKCERT had received 1,536 applications from Open group, Secondary School group and Primary School group. A professional judge panel selected winners with good attractive designs (See Figure 7).

Figure 7. Champion entries of Open, Secondary School and Primary School Group (from left to right)

We organized the 2-day Information Security Summit 2015 with other information security organizations and associations in October 2015, inviting local and international speakers to provide insights and updates to local corporate users.

We jointly organized a seminar of “Transaction Security of Mobile Apps in Hong Kong Study” with other information security organizations and associations in November 2015, sharing research study conducted by HKCERT to mobile apps owners and developers.

3.2 TRANSITS CSIRT Training

HKCERT brought the first TRANSITS program to Hong Kong. HKCERT had organized a 3-day CSIRT training in December 2015. The workshop informs trainees with the global perspective of CSIRT and local knowledge of security incident coordination. There are 11 and 3 participators come from Hong Kong and Macau respectively.

3.3 Speeches and Presentations

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

3.4 Media promotion, briefings and responses

- HKCERT published two advertorials in November 2015 to promote the public seminar and the graphics design contest.
- HKCERT published weekly column articles in Hong Kong Economic Times 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 Malaysia and delivered a workshop on IFAS
- Participated in the FIRST AGM and Conference in Berlin and delivered talk on cyber threat intelligence collection and analysis systems; participated in the Annual Meeting for CSIRTs with National Responsibility in Berlin and shared in the panel discussion the future of CERTs.
- Participated in the APCERT Drill (March 2015) and acted as member of the Organizing Committee and the Exercise Control team. The theme of the drill this year was “Cyber Attacks beyond Traditional Sources”. The drill was a great success with 25 APCERT teams from 19 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.

HKCERT promotes the Decision Support and Monitoring System (DSMS) to other CERTs. AusCERT started to use DSMS and had developed some modules to DSMS.

HKCERT collaborated with APNIC closely in taking down bad reputation ASNs whose owners were suspicious and may not provide proper contact information.

4.2 Local Collaboration

GovCERT.HK was established April 2015. HKCERT, together with MOCERT, sponsored GovCERT.HK to join APCERT and FIRST membership, HKCERT had paid a visit to the GovCERT.HK office for this purpose.

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

- Continued to work closely with the government (GovCERT.HK since April 2015) 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 2015, HKCERT had worked with ISPs to clean up Citadel, ZeroAccess, GameoverZeus, Pushdo, Ramnit and XcodeGhost botnet machines in Hong Kong.
- 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 CNCERT Visit

HKCERT had visited CNCERT/CC in China in December of 2015. The mission of this tour was to understand and discuss with CNCERT their business services, the enabling factors and the lesson learnt. 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

5.2 Advisory Group Meeting

HKCERT had held the Advisory Meeting in July of 2015. The meeting provides solicit inputs from the advisors on the development strategy of HKCERT.

5.3 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.

5.4 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.

5.5 Year Ender press briefing

HKCERT organized a year ender press briefing to media in January 2016 to report on information security status of 2015, 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 8. 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 2015, 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 2016/2017. 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

In 2015, 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 2015, 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, phishing, 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 2016.

-- END --