# ANNUAL REPORT 2016

香港電腦保安事故協調中心

Hong Kong Computer Emergency

Response Team Coordination Centre

Hong Kong Productivity Council

# HKCERT Annual Report 2016

## 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 2016, HKCERT had handled 6,058 security incidents which was 23% increase of the previous year (see Figure 1).

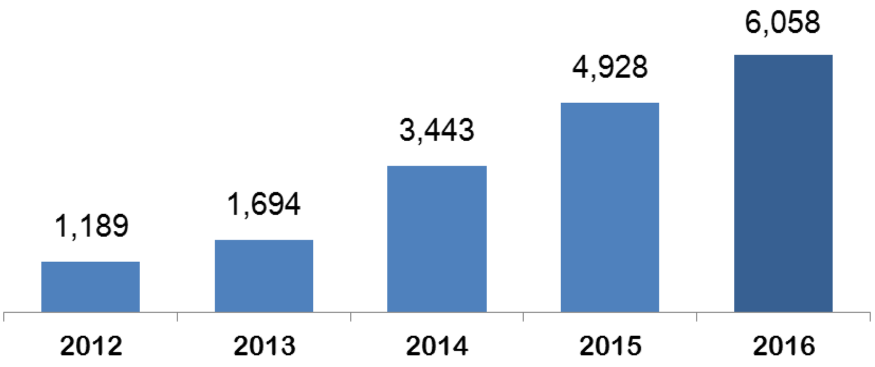


*Figure 1. Incident Reports Handled by HKCERT*

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 89% of the total number of security incidents.

Two major categories of security incidents, Botnet (2,018 cases) and Phishing (1,957 cases) remained at similar level as in the previous year (see Figure 2).

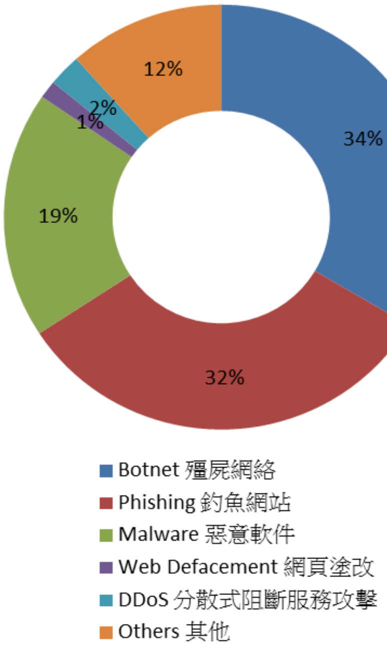


*Figure 2. Distribution of Incident Reports in 2016*

The number of malware infection incident reports rose sharply by 247% in 2016 (see Figure 3.) These case were mainly due to XcodeGhost contaminated mobile app and ransomware. Ransomware case had grown rapidly by 506% (see Figure 4) with Locky, CryptXXX and Zepto as the most prominent ones..

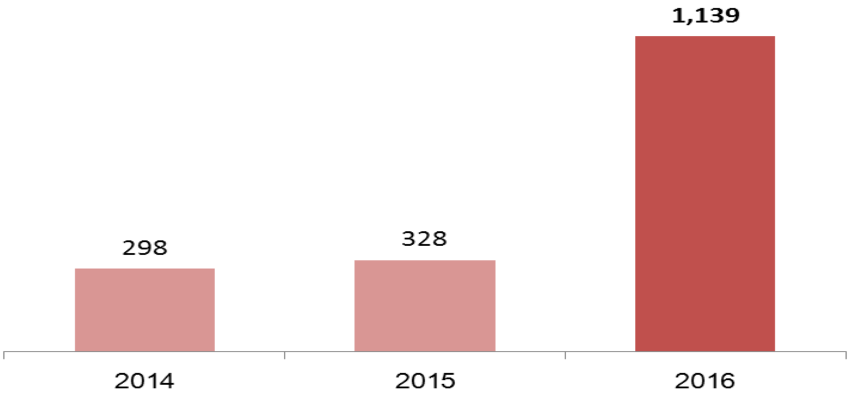


*Figure 3. Number of Malware Incident Reports in the past 3 years*

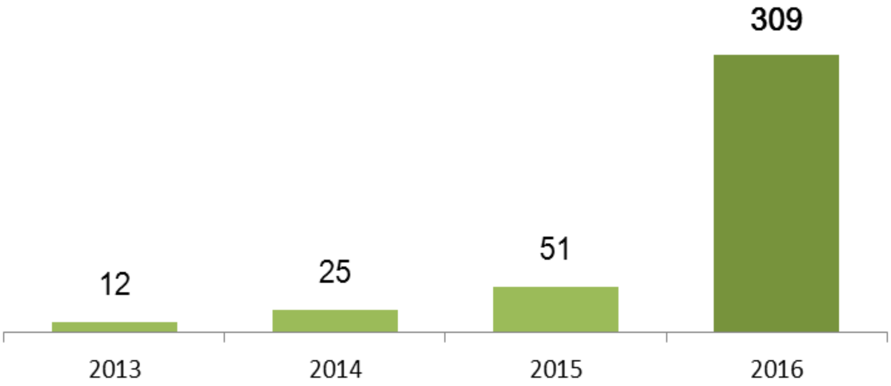


*Figure 4. Number of Ransomware Incident Reports in the past 4 years*

## 2.2 Watch and Warning

During the period from January to December of 2016, HKCERT published 336 security bulletins (see Figure 5) on the website. In addition, HKCERT have also published 101 blogs, including security advisories on SSL/TLS Protocols Security, phishing scam, banking Trojan, ransomware, vulnerabilities on Android devices, DDoS by IoT devices and data leakage. HKCERT also published the "best security reads of the week" every week to inform the public of good security articles.

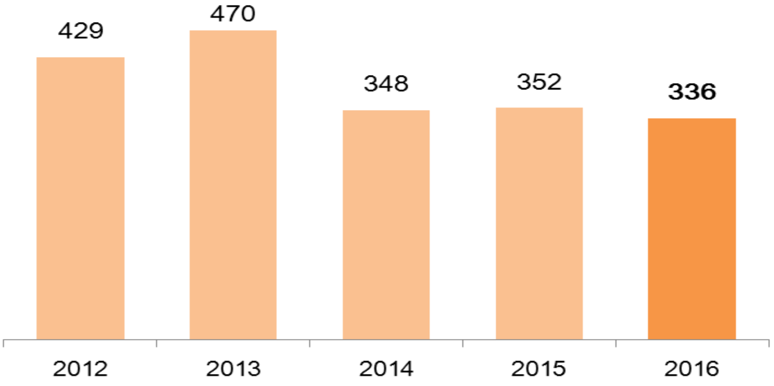


*Figure 5. HKCERT Published Security Bulletins*

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 used 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 a way to verify the effectiveness of the security incident response. For example, Figure 6 showed the trend of bot related security events slightly decreasing from 5,626 in Q4 2015 to below 5,000 in 2016. Figure 7 showed the trend of top 5 botnet families in the past year. The overall decreasing trend of botnet families, except a new botnet family Mirai in Q4 1016, reflected the effectiveness of the botnet takedown operation.

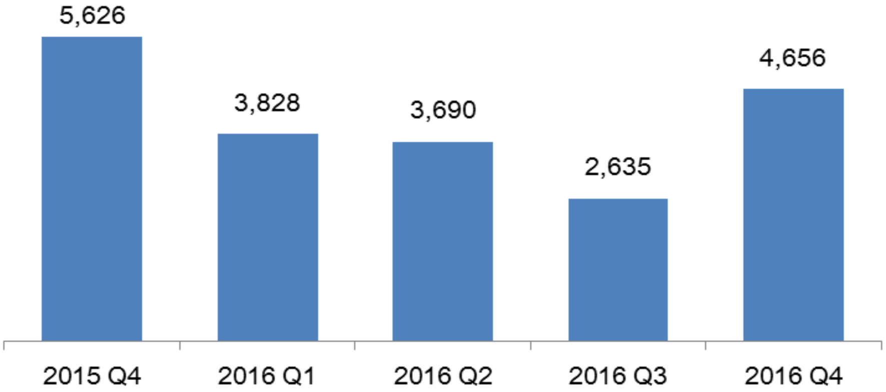


*Figure 6. Trend of Bot related security events in the past year*

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

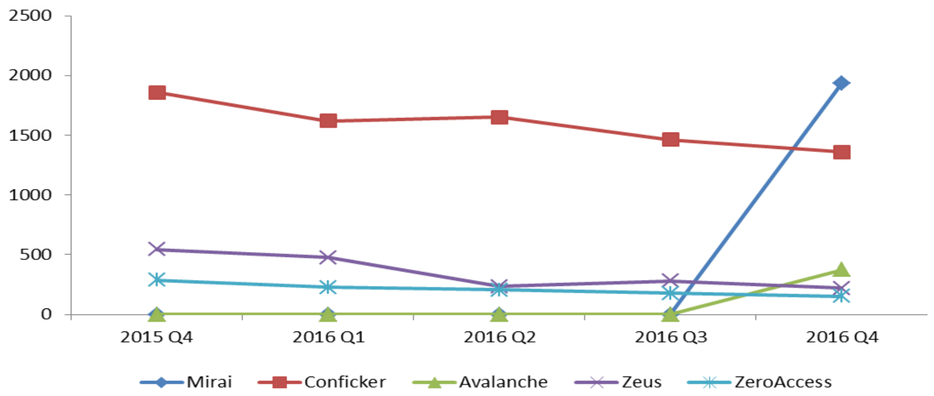


*Figure 7. Trend of Top 5 Botnet Families in the past year*

*(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. (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).

- HKCERT had published 50 weekly column articles in a local Chinese newspaper (Hong Kong Economic Times) to raise the cyber security awareness of business executives.
  (see https://hkpc.org/en/corporate-info/media-centre/media-focus#1).

## 3. Events organized and co-organized

### 3.1 Seminars, Conference and Meetings

HKCERT jointly organized the “Build a Secure Cyberspace 2016” campaign with the Government and Hong Kong Police Force. The campaign involved public seminars, and a mascot design contest. Two public seminars were organized in May and November 2016.

For the graphic design contest, HKCERT had received over 2,000 applications from Open group, Secondary School group and Primary School group. A professional judge panel selected winners with good attractive designs (See Figure 8).

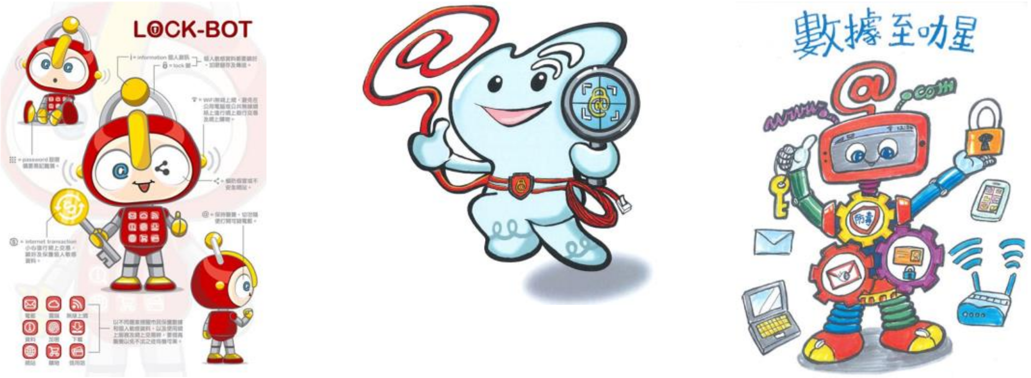
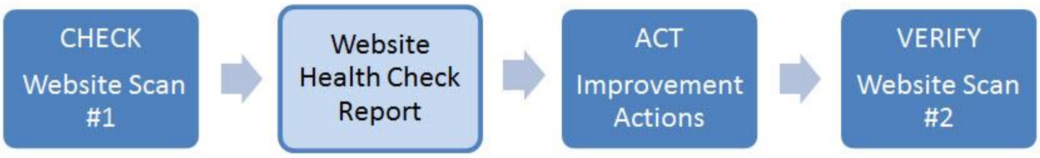


*Figure 8. Champion entries of Open, Secondary School and Primary School Group (from left to right)*

We organized the 2-day Information Security Summit 2016 with other information security organizations and associations in September 2016, inviting local and international speakers to provide insights and updates to local corporate users.

We organized a SME Free Web Security Health Check Pilot Scheme to promote SMEs to secure their website using the "Check-Act-Verify" approach. Free website scanning and advisory was provided to SMEs joining the scheme. A public seminar was organized to debrief the findings of SME website security status in the scheme.



### 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 an advertorial in November 2016 to promote the public seminar and the mascot design contest.
- 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 Japan and delivered a talk on DSMS.
- Participated in the FIRST AGM and Conference in Seoul; participated in the Annual Meeting for CSIRTs with National Responsibility in Seoul.
- Participated in the APCERT Drill (March 2016) and acted as member of the Organizing Committee and the Exercise Control team. The theme of the drill this year was "An Evolving Cyber Threat and Financial Fraud". The drill was a great success with 26 APCERT teams from 20 economies, and 6 economies of OIC-CERT participating.
- Participated in the CNCERT Annual Conference 2016 in ChengDu.
- 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 Vienna, Austria
- Represented APCERT in the Advisory Council of DotAsia Organization

HKCERT signed an MOU with CNCERT to further collaboration in incident response, information exchange and project cooperation.

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.

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

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

- Continued to work closely with the government (GovCERT.HK) and law enforcement agency, and held meetings to exchange information and to organize joint events regularly. In 2016, HKCERT was a coorganizer and a member of the judge panel member in the first Cyber Security Professionals Awards organized by Hong Kong Police Force.
- 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 2016, HKCERT had worked with ISPs to clean up Citadel, ZeroAccess, GameoverZeus, Pushdo, Ramnit and XcodeGhost botnet machines in Hong Kong. In 2016 September, HKCERT organized a Cyber Security Symposium "Challenges to Cyber Resilience for Internet Infrastructure Providers".
- 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 Advisory Group Meeting

HKCERT had held the Advisory Meeting in August of 2016. The meeting provides solicit inputs from the advisors on the development strategy of HKCERT.

### 5.2 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 previous 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 joined the Cyber Green project initiated by JPCERT/CC to explore development of useful metrics for measuring cyber health.

### 5.5 Year Ender press briefing

HKCERT organized a year ender press briefing to media in January 2017 to review cyber security 2016, and provided outlook to 2017 to warn the public for better awareness and preparedness. It received very good press coverage.

*Figure 9. HKCERT at the Year Ender press briefing.*

## 6. Future Plans

### 6.1 Strategy

“Proactivity”, “Share to Win” and “Security is not an Island” are the strategic directions of HKCERT which would work closer with other CERTs and security organizations to build a more secure Hong Kong and Internet.

### 6.2 Funding

HKCERT had secured Government funding to provide the basic CERT services in 2017/2018. 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 infrastructure to increase the efficiency of information search and sharing. HKCERT was developing automation tools to enhance the incident response process.

## 7. Conclusion

In 2016, HKCERT was 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.

With the Internet security facing more crises from crime-as-a-service, ransomware, phishing, IoT attacks 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 --**