



# ANNUAL REPORT 2018

---

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 2018

### 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 organisation in Hong Kong, has operated the centre since then.

#### 1.2 Organisation 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, two Consultants and six Security Analysts and one Assistant Project Manager.

#### 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 2018, HKCERT had handled 10,081 security incidents which was 55% increase of the previous year (see Figure 1).

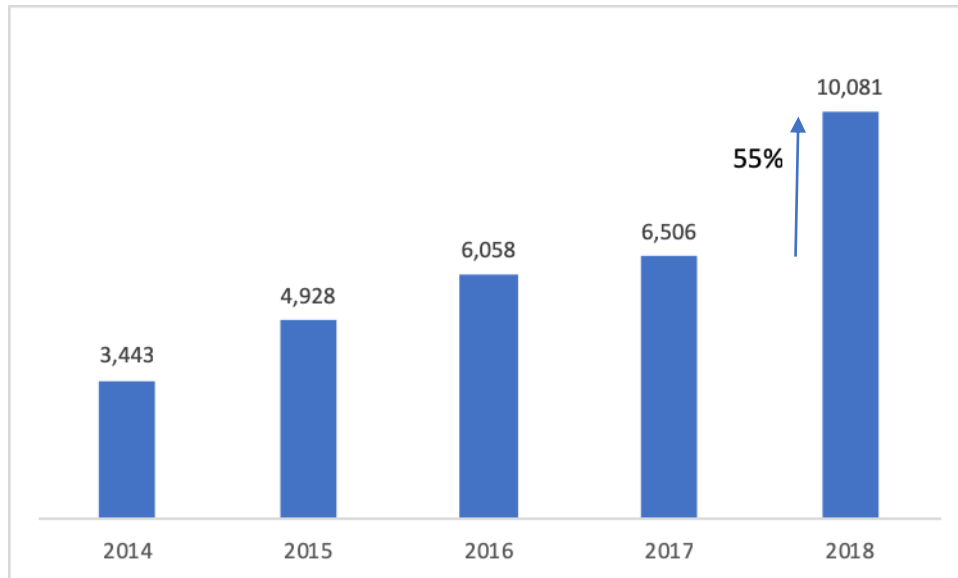


Figure 1. Incident Reports Handled by HKCERT

The 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 organisations. Referral cases accounted for 95% of the total number of security incidents.

Two major categories of security incidents, Botnet (3,783 cases) and Phishing (2,101 cases) remained at similar level as in the previous year (see Figure 2).

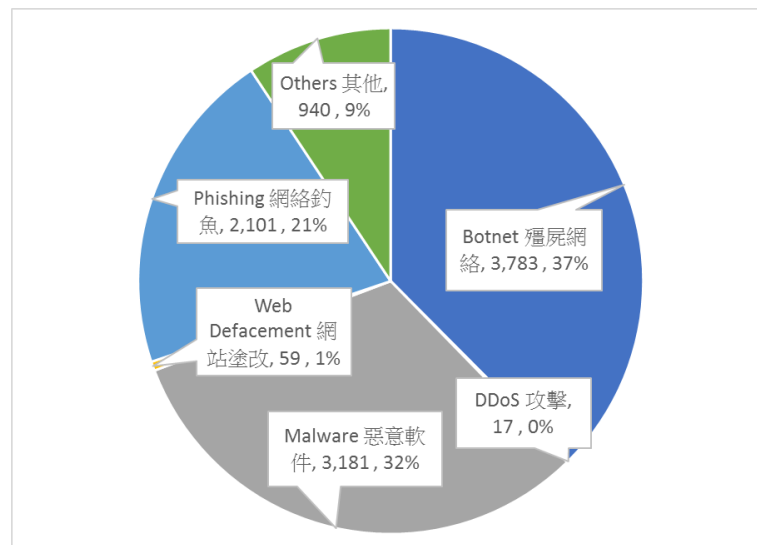


Figure 2. Distribution of Incident Reports in 2018

The number of malware infection incident reports rose sharply by 56% in 2018 (see Figure 3.) These cases were mainly due to WannaCry sinkhole detections (bot-Wannacry) and XcodeGhost contaminated mobile apps. Among all malware reports, despite fewer ransomware incident reports (114 cases) were made to HKCERT last year, there were 2,426 bot-Wannacry cases, which doubled the number 1,210 of 2017.

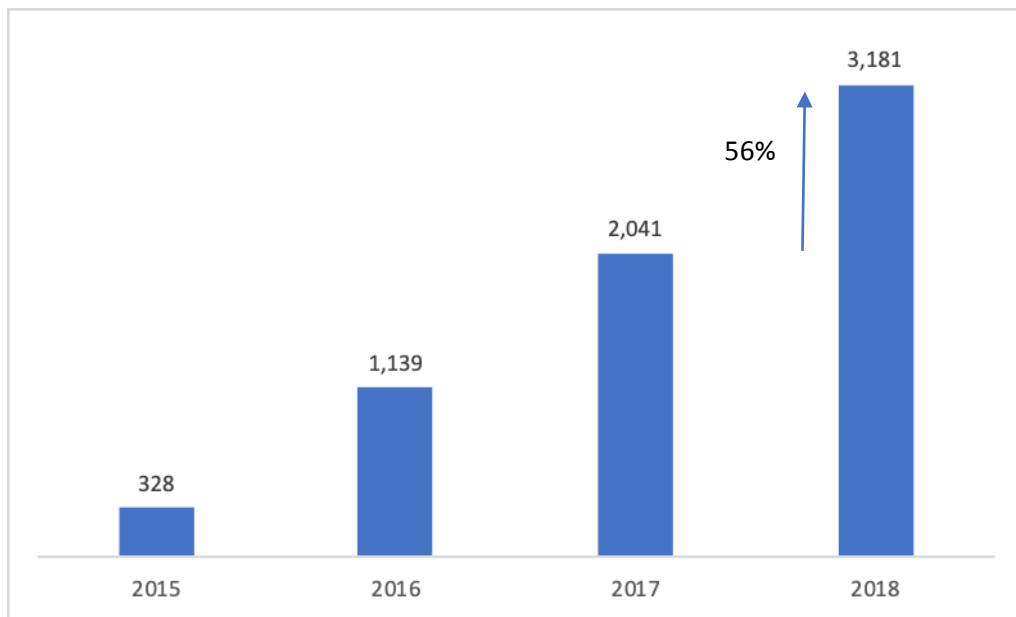


Figure 3. Number of Malware Incident Reports in the past 4 years

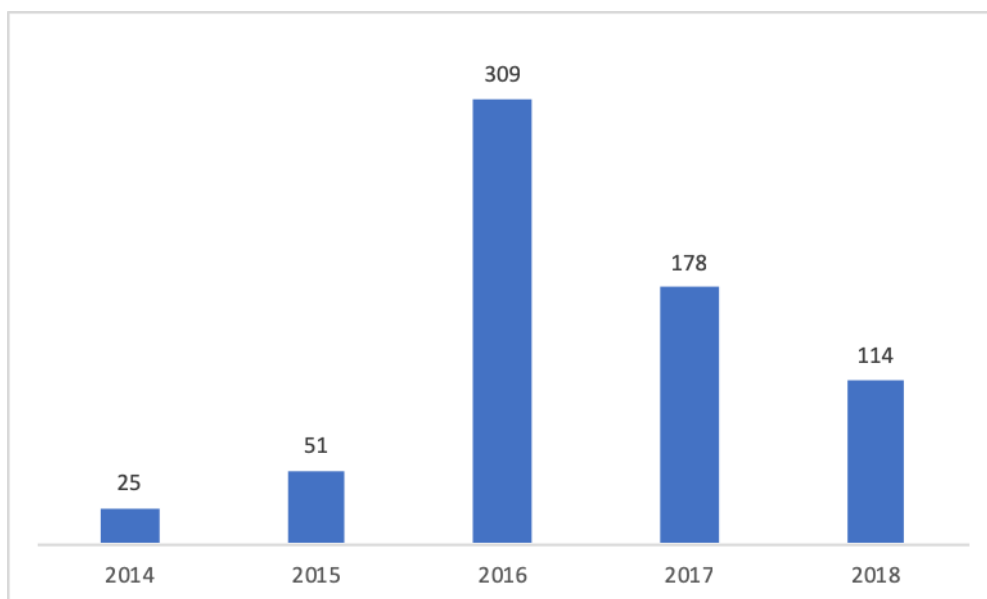


Figure 4. Number of Ransomware Incident Reports in the past 5 years

## 2.2 Watch and Warning

During the period from January to December of 2018, HKCERT published 240 security bulletins (see Figure 5) on the website. In addition, HKCERT have also published 99 blogs, including security advisories on DDoS extortion, marketing adware, smart device installation, ransomware, IoT Botnet, remote desktop service risk, third party plugins, etc. HKCERT also published the “best security reads of the week” every fortnight to inform the public of good security articles.

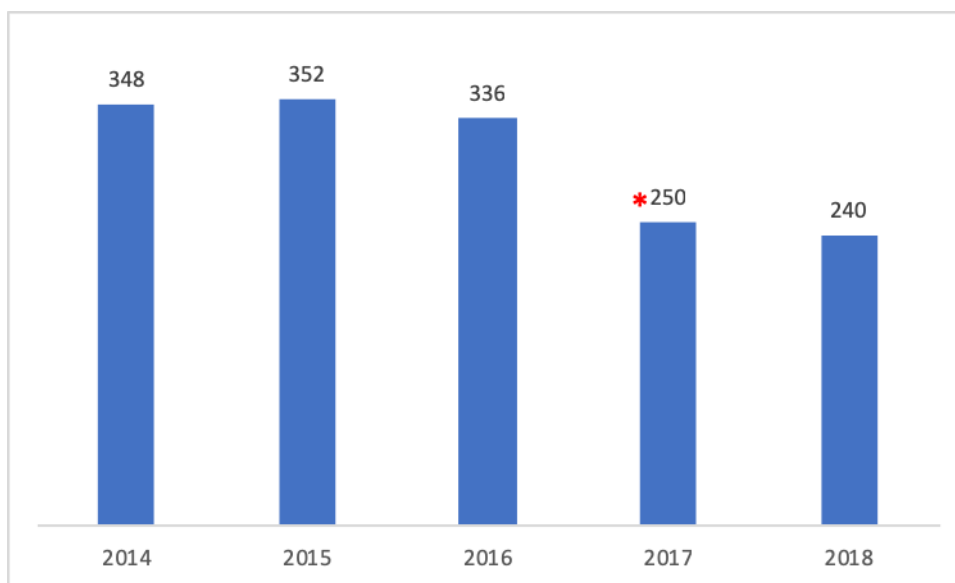


Figure 5. HKCERT Published Security Bulletins

\*The drop of Security Bulletins was mainly due to consolidation of MS & Adobe security bulletins

HKCERT used the centre website ([www.hkcert.org](http://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 was on the rise in the past year (from 4,690

in Q4 2017 to 7,307 in Q4 2018), largely attributed to the significant rise of Mirai events as depicted in Figure 7.

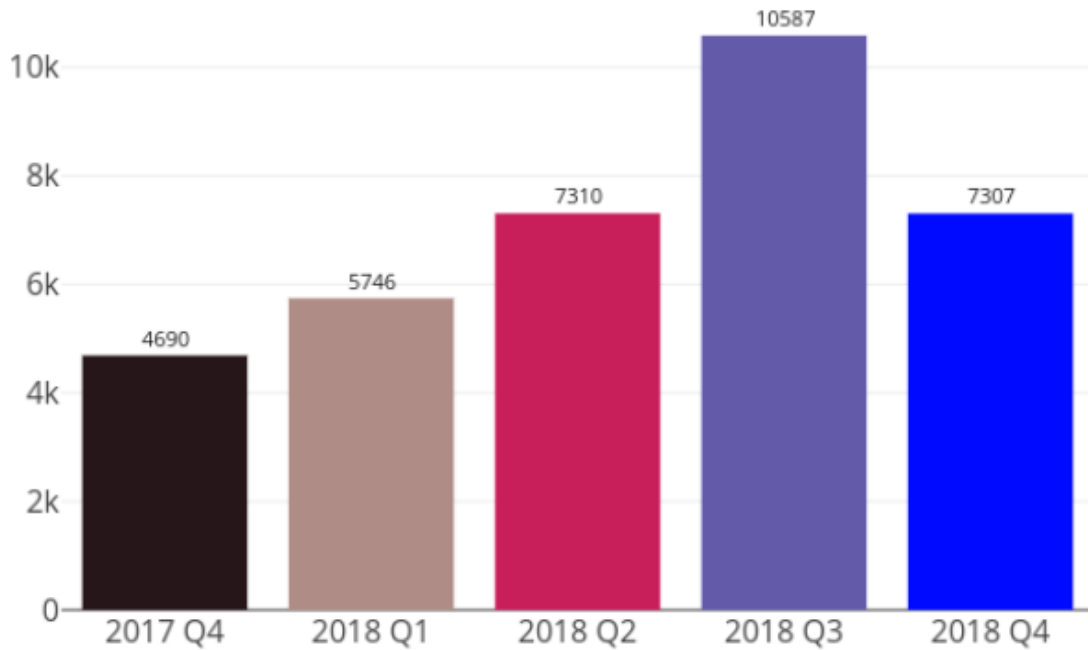


Figure 6. Trend of Bot related security events in the past year

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

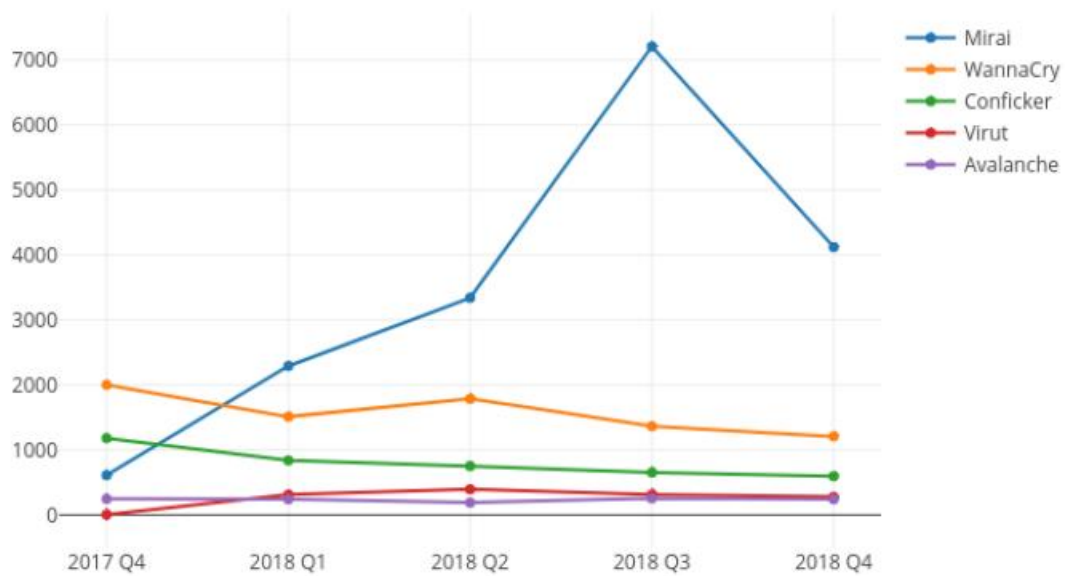


Figure 7. Trend of Top 5 Botnet Families in the past year

(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>).



- 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 organised and co-organised

#### 3.1 Seminars, Conference and Meetings

HKCERT jointly organised the “Build a Secure Cyberspace 2018” campaign with the Government and Hong Kong Police Force. The campaign involved public seminars, and a 1-Minute Video Ad Contest. Two public seminars were organised in April and September 2018.

For the 1-Minute Video Ad Contest, HKCERT had received about 55 applications from Open Category, Family Category, Secondary School and Primary School Category. A professional judge panel selected winners with most innovative and impressive videos (See Figure 8).

##### Winning Entries of Primary School Category



Champion -  
畢可疑  
Kwan Hei Man, Yeung Wai Chun,  
Chuah Ching Huen, Lee Pui Ki,  
Hung Ming Yan, Chow Ka Wai  
(S.K.H. St. Michael's Primary School)

##### Winning Entries of Secondary School Category



Champion -  
沽名釣魚 一黑千金  
Sze To Wun Chung,  
Tsang Chun Lung,  
Lam Chin Cheung, Cheng Chak Ho,  
Ip Chak Yan, Tang Yun Kuen  
(S.K.H. Bishop Baker Secondary School)

##### Winning Entries of Open Category



Champion -  
朋友想“點”?  
Chan Ka Ho

##### Winning Entries of Family Category



Champion -  
網上購物意外多，認清網站纒趣多  
Chan Ka Lok, Hadrian Chan

Figure 8. Champion entries of Primary School, Secondary School, Open and Family Category



See this link to view those winning entries online:

<https://www.cybersecurity.hk/en/contest-2018-prize.php>

We co-organised the 2-day Information Security Summit 2018 with other information security organisations and associations in September 2018, 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 Proactive approach to promote awareness for different sectors in HK**

HKCERT proactively approached several sectors in HK to promote cyber security awareness, e.g. travel industry, retail and securities, etc.

### **3.4 Media promotion, briefings and responses**

- HKCERT published an advertorial in September 2018 to promote the public seminar and the 1-Minute Video Ad 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 Shanghai
- Participated in the FIRST Meeting and National CSIRT Meeting in Kuala Lumpur
- Participated in the CNCERT Conference in Beijing
- Participated in the AusCERT Conference in Gold Coast
- Participated in the HITCON Community in Taipei
- Participated in International honeypot initiatives, including joining the Tsubame project of JPCERT/CC and The Honeynet Project.
- Participated in (ISC)2 APAC Security Congress

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 organisations in different areas. Some examples:

- HKCERT continued to work closely with the government (GovCERT.HK) and law enforcement agency and held meetings to exchange information and to organise joint events regularly.
- To promote cyber security information sharing among industries in Hong Kong, the Hong Kong SAR Government launched the Cyber Security Information Sharing platform called ‘Cybersec Infohub’. Over 100 Information Security companies and critical infrastructure organisations were invited to join the platform. Cyber security information and intelligence were shared among the members. HKCERT joined as a member of the Programme. HKPC, the parent organisation of HKCERT, is the programme manager of the Programme.
- HKCERT 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 was a judge panel member of the Cyber Security Professionals Awards organised by the Hong Kong Police.
- HKCERT continued to maintain the Information Security Advisory and Collaboration (ISAC) Mailing list with the Internet infrastructure organisations, and advised on latest information security issues through the list.
- HKCERT also liaised with critical infrastructure sector and had delivered awareness briefings to these organisations for better protecting the security environment of Hong Kong; created the Information Security Advisory and Collaboration (ISAC-CI) Mailing list with the critical infrastructure organisations, 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 November of 2018. The meeting solicited inputs from the advisors on the development strategy of HKCERT.

### 5.2 Three Year Strategic Plan

HKCERT prepared its rolling Three Year Strategic Plan based on inputs from Advisory Group, the Strategy and Service Review Report, the previous CERT Study Tour and discussion 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 publicised 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 organised a year ender press briefing to media in January 2019 to review cyber security 2018 and provided outlook to 2019 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 organisations to build a more secure Hong Kong and Internet.

### **6.2 Funding**

HKCERT had secured Government funding to provide the basic CERT services in 2019/2020. 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 2018, there were data breach cases in airlines and telecommunication companies in Hong Kong. Process flaws were also exploited by fraudsters in registration of third-party wallets in mobile payment. Besides promoting public information security awareness, HKCERT also urged enterprises to adopt “Security by Design” and enhance risk management process.

The cross-border collaboration and intelligence driven response continued to improve the proactiveness and effectiveness of incident response. HKCERT has seen the immense power of collaboration and would invest more to further this success.

With the Internet security facing more crises from financially motivated cyber crimes, Internet of Thing (IoT) attacks, more use of mobile payment apps, more regulation for security and privacy and supply chain attacks, HKCERT expects 2019 would be continuously a challenging year.

-- END --