ANNUAL REPORT 2017

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 2017

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 2017, HKCERT had handled 6,506 security incidents which was 7% increase of the previous year (see Figure 1).

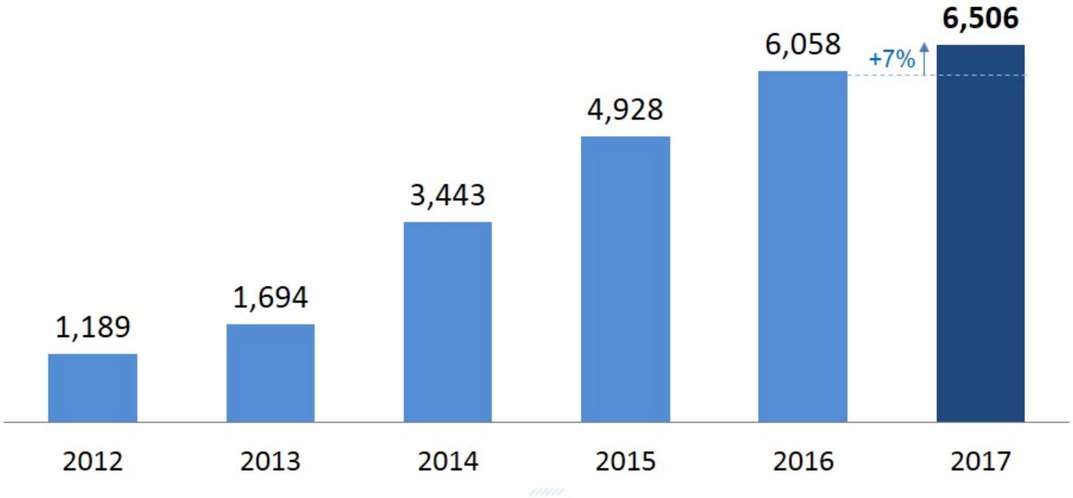
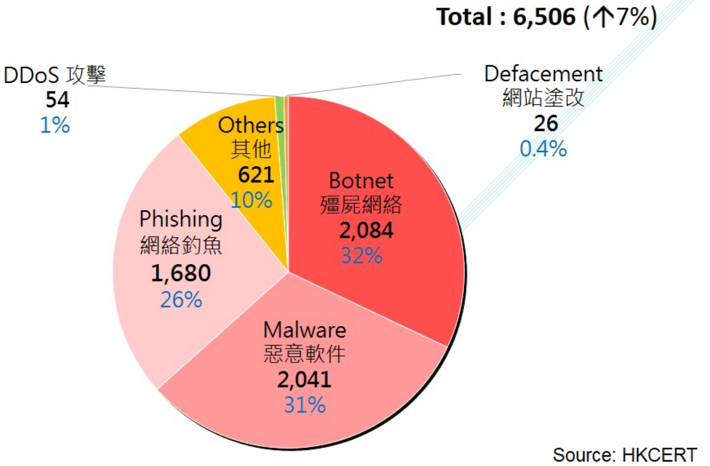


Figure 1. Incident Reports Handled by HKCERT

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 organizations. Referral cases accounted for 91% of the total number of security incidents.

Two major categories of security incidents, Botnet (2,084 cases) and Phishing (1,680 cases) remained at similar level as in the previous year (see Figure 2).



Source: HKCERT

Figure 2. Distribution of Incident Reports in 2017

The number of malware infection incident reports rose sharply by 79% in 2017 (see Figure 3.) These cases were mainly due to WannaCry sinkhole detections and XcodeGhost contaminated mobile apps. Among all malware reports, despite fewer Ransomware incident reports (178 cases) were made to HKCERT last year, there were 1,210 bot-Wannacry cases. These involved large number of computers being infected by the notorious Wannacry ransomware that rocked the world last May, but encryption was yet to be triggered.

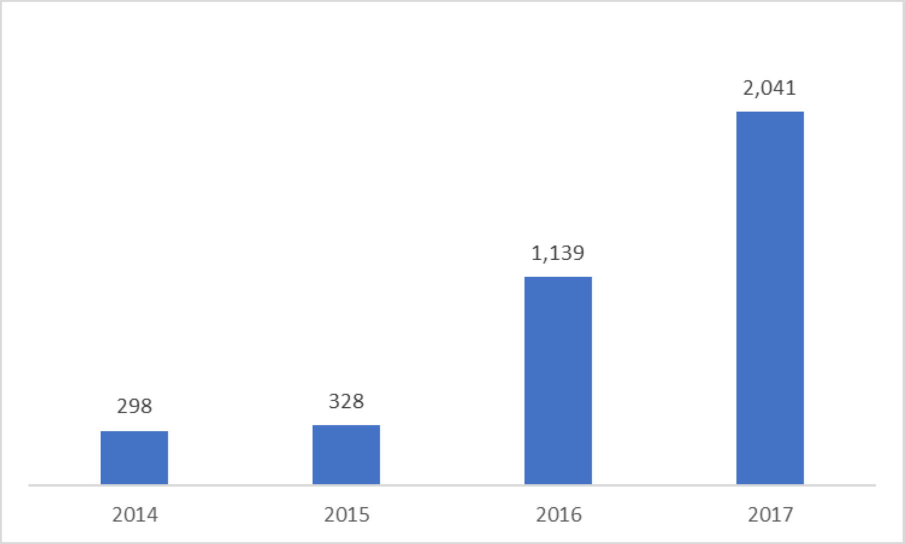


Figure 3. Number of Malware Incident Reports in the past 4 years

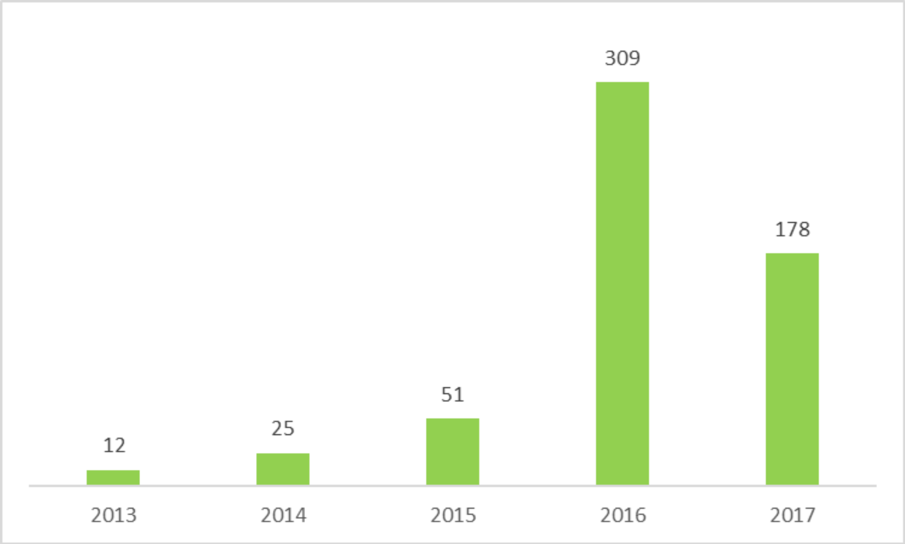


Figure 4. Number of Ransomware Incident Reports in the past 5 years

2.2 Watch and Warning

During the period from January to December of 2017, HKCERT published 250 security bulletins (see Figure 5) on the website. In addition, HKCERT have also published 110 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 week to inform the public of good security articles.

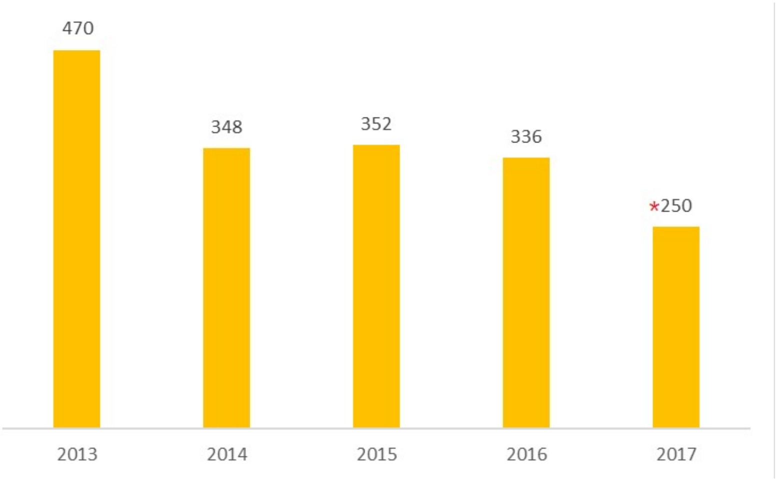


Figure 5. HKCERT Published Security Bulletins

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

HKCERT used the centre website (www.hkcert.org), 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 maintains similar figures (from 4,656 in Q4 2016 to 4,690 in 2017). But the figures have included WannaCry sinkhole which maintains around 2,000. Mirai got significant decrease after 1 year of botnet clean operation.

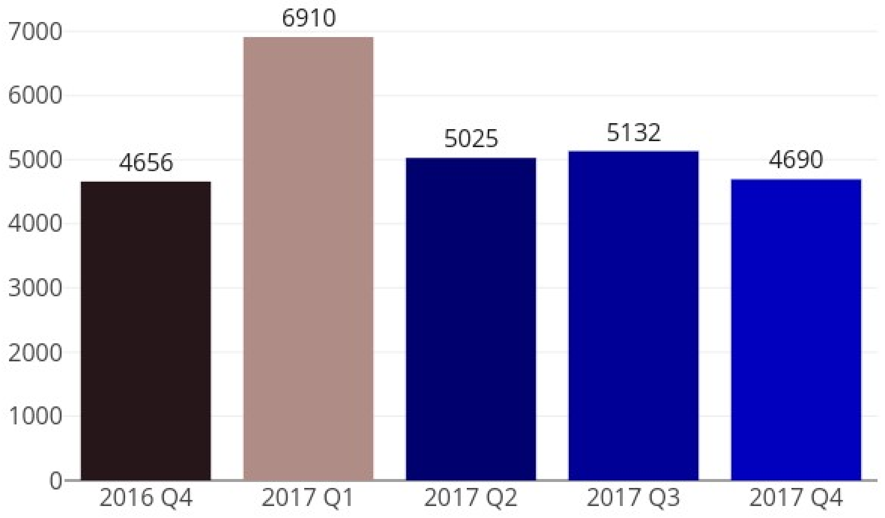


Figure 6. Trend of Bot related security events in the past year

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

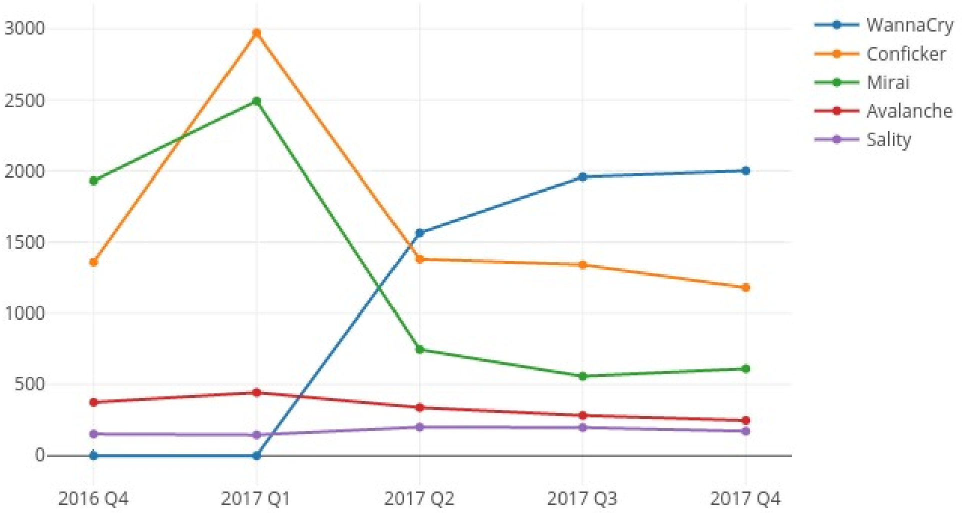


Figure 7. Trend of Top 5 Botnet Families in the past year

(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 1-Page Comic Drawing Contest. Two public seminars were organized in April and September 2017.

For the graphic design contest, HKCERT had received about 1,200 applications from Open group, Secondary School group and Primary School group. A professional judge panel selected winners with good attractive drawing (See Figure 8).

公開組冠軍
網絡安全大師
作品：網絡安全大師
得獎者：劉滋林
中學組冠軍
鼠竊狗偷講拜拜 防犯入侵責無旁貸
作品：鼠竊狗偷講拜拜 防犯入侵責無旁貸
得獎者：高苡琳 (嘉諾撒聖方濟各書院)
小學組冠軍
網絡安全做到足，一家上網好輕鬆
作品：網絡安全做到足，一家上網好輕鬆
得獎者：楊民逸 (聖文德天主教小學)

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

We organized the 2-day Information Security Summit 2017 with other information security organizations and associations in August 2017, 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 2017 to promote the public seminar and the 1-Page Comic Drawing 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 New Delhi
- Participated in the FIRST Meeting and National CSIRT Meeting in Puerto Rico
- Participated in the CNCERT Conference in Qingdao
- Participated in the AusCERT Conference in Gold Coast
- 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 organizations 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 organize joint events regularly. In 2017, HKCERT was a co-organizer and a member of the judge panel member in the 2nd Cyber Security Professionals Awards organized by Hong Kong Police Force.
- To combat worsening ransomware cyber attacks, HKCERT and the government GovCERT.hk jointly launched a "Flight Ransomware Campaign" on 5 September 2017 to strengthen the readiness of Hong Kong businesses and general public against ransomware attacks. Riding on the popularity of social media and mobile technologies, the new campaign includes the creation of a Facebook page "Ransomware Intelligence Portal" (www.facebook.com/ransomware.hk) where HKCERT teams up with major international IT and cyber security companies for early sharing of intelligence of global trends and insights about ransomware, security alerts and training information with the public. In addition, the public will have access to free anti-malware software with real-time protection, provided by cyber security partners of the campaign.
- 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. In 2017, HKCERT had worked with ISPs to develop a "Service Provider Interconnection, Routing and Information Security Best Practices" (SPIRITS) guideline. A symposium was also organized with HKISPA in December to promote the best practice guideline. More activities will be expected in 2018 to engage ISPs in Hong Kong.
- HKCERT continued to Maintain the Information Security Advisory and Collaboration (ISAC) Mailing list with the Internet infrastructure organizations, and advised on latest information security issues through the list
- HKCERT also 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 September of 2017. 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 2018 to review cyber security 2017, and provided outlook to 2018 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 2018/2019. 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 2017, HKCERT was active in promoting public awareness of ransomwares and their impact on corporations particular SMEs. 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 2018 would be continuously a challenging year.

-- END --