ANNUAL REPORT 2019

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 2019

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 2019, HKCERT had handled 9,458 security incidents which was 6% decrease of the previous year (see Figure 1). Referral cases accounted for 92% of the total number of security incidents.

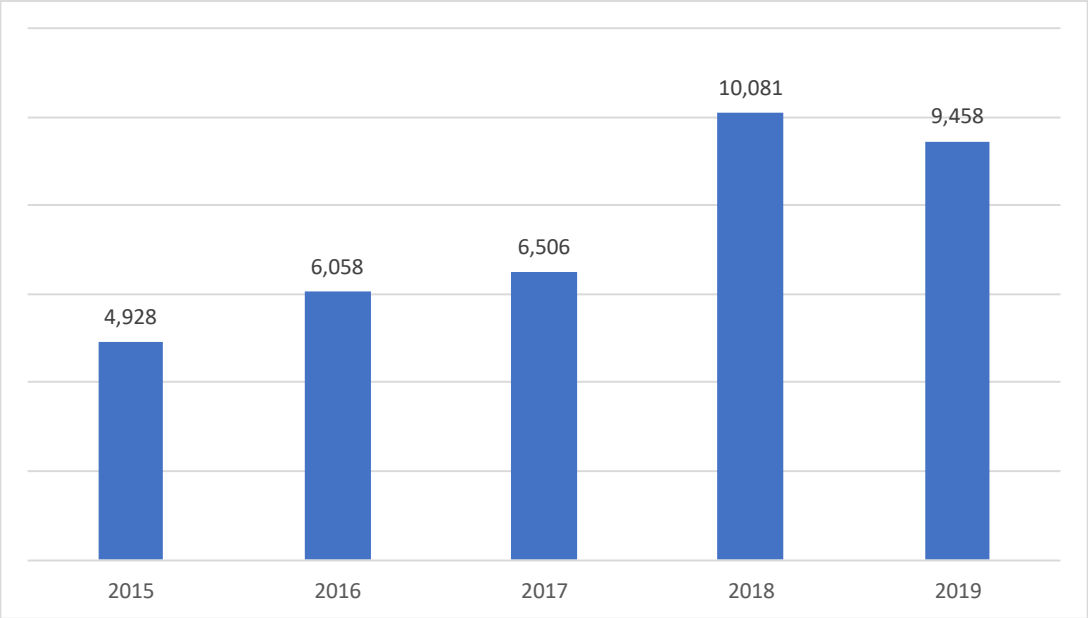


Figure 1. HKCERT Security Incident Reports

While the number of overall security incidents handled by HKCERT reported a 6% year-on-year drop in 2019, totally 9,458, Botnet (4,922 cases or 52%) and phishing websites (2,587 cases or 27%), two principal sources of reports, still went up 30% and 23% respectively which were mainly attributed to rise in financial crime-related Botnets and phishing targeting financial organizations and enterprises. On the other hand, malware reports (1,219 cases or 13%) fell 62% as more malware stayed stealthy after infection and ransomware targeted more on global enterprises for higher return instead of massive untargeted attacks. (see Figure 2).

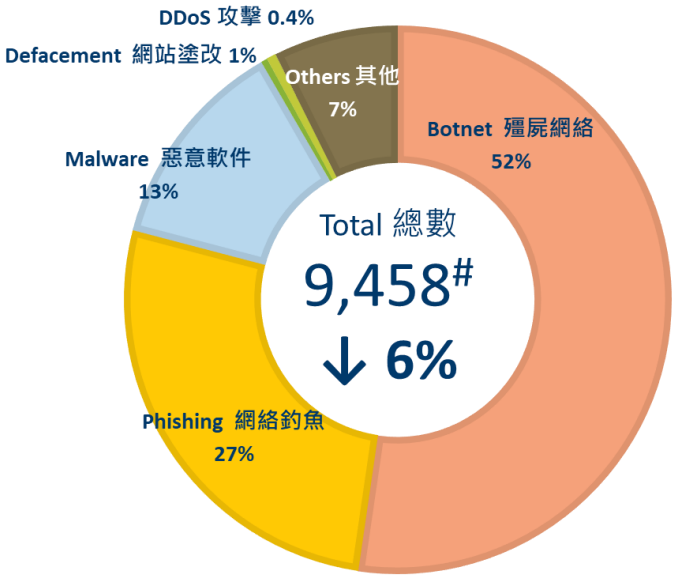


Figure 2. Distribution of Incident Reports in 2019

2.2 Watch and Warning

During the period from January to December of 2019, HKCERT published 273 security bulletins (see Figure 3) on the website. In addition, HKCERT have also published 48 blogs, including security advisories on GDPR, ransom email attacks, IoT security risks at home, ransomware, webcam etc.

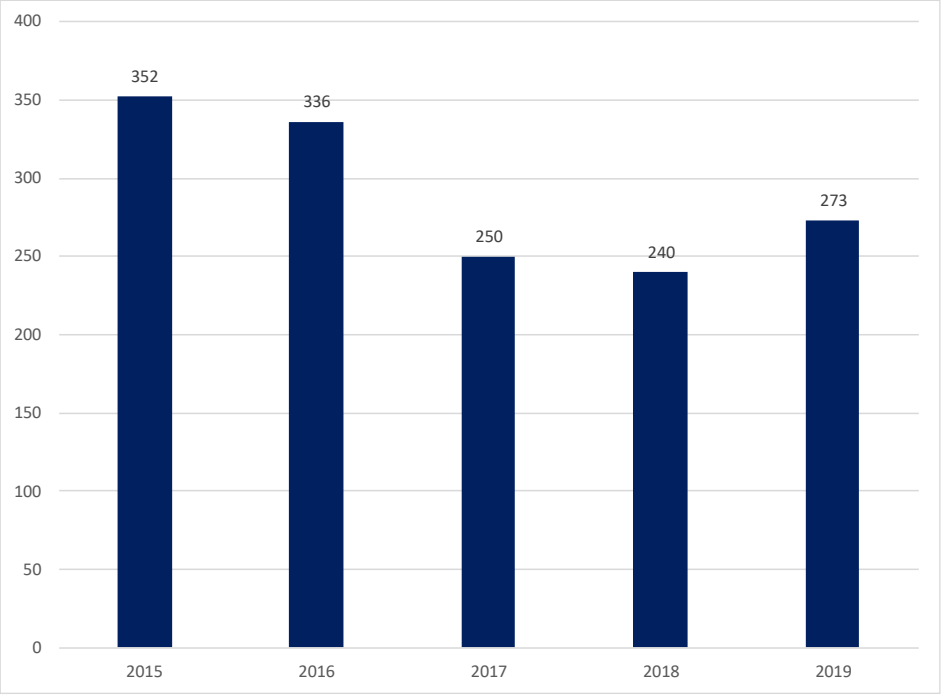


Figure 3. HKCERT Published Security Bulletins

The drop of Security Bulletins in 2017 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 4 showed the number of bot-related in Hong Kong network reached a record high of 11,554 in 2019 Q2 and finally dropped to 6,831 in Q4 2019), largely attributed to the significant rise of Mirai events as depicted in Figure 5.

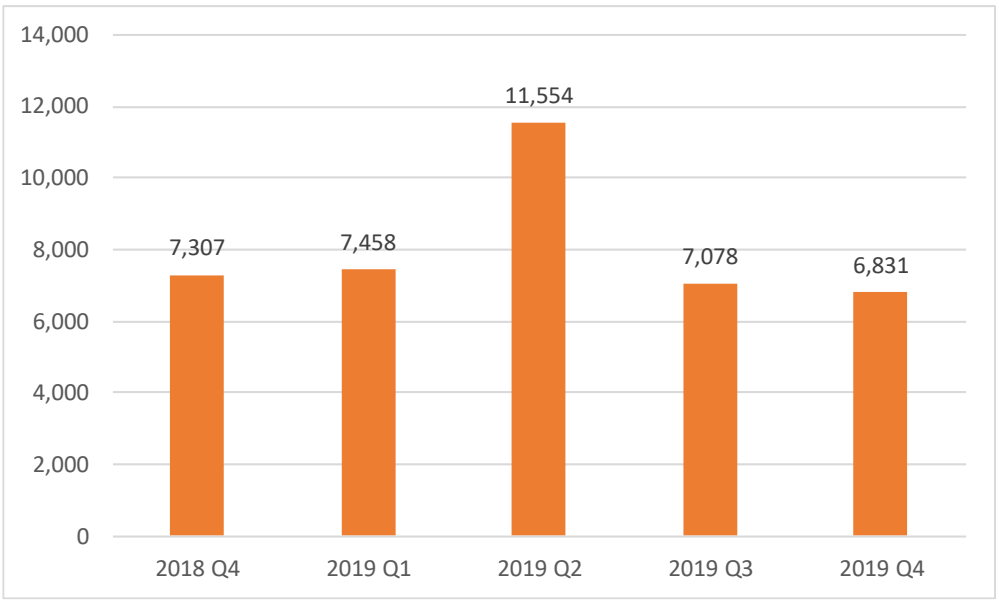


Figure 4. Trend of Bot related security events in the past year

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

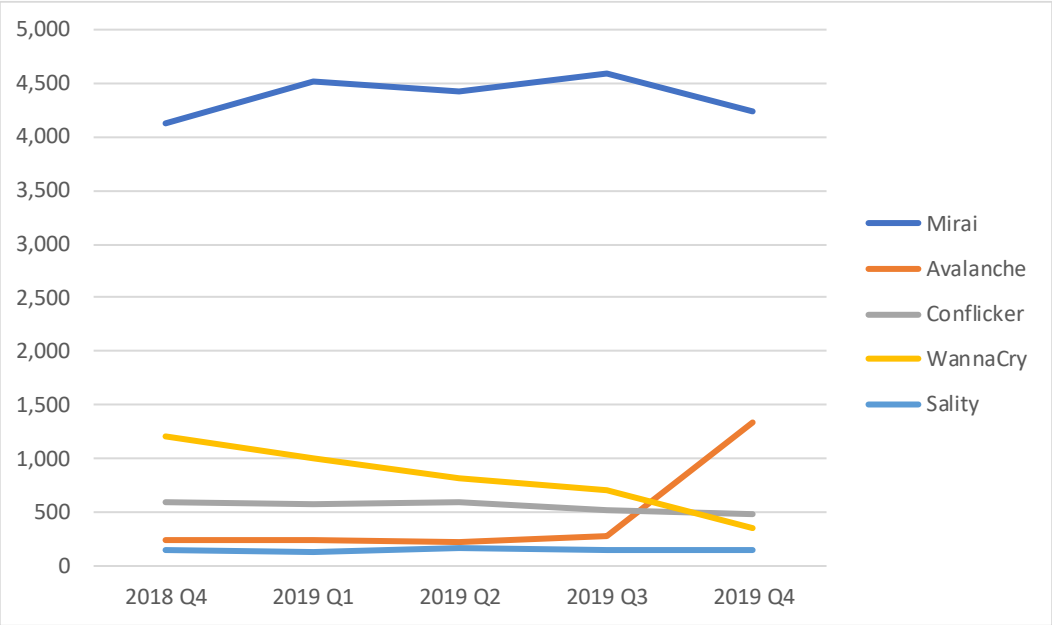


Figure 5. Trend of Top 5 Botnet Families in the past year

(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 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 organised and co-organised

3.1 Seminars, Conference and Meetings

HKCERT jointly organised the “Build a Secure Cyberspace 2019” campaign with the Government and Hong Kong Police Force. The campaign involved public seminars, and a Poster Design Contest. Two public seminars were organised in May and September 2019.

For the Poster Design Contest, HKCERT had received about 546 applications from Open Group, Family Group, Secondary School and Primary School Group. A professional judge panel selected winners with most creative and outstanding poster design (See Figure 6).

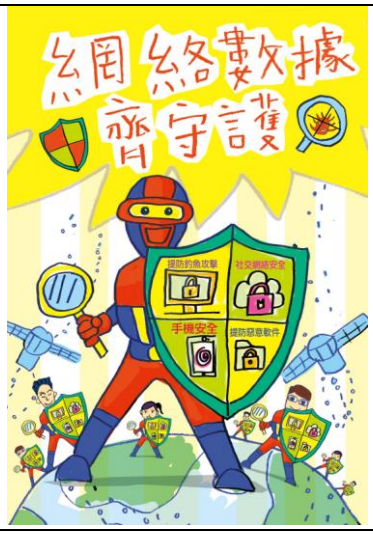
<table>
<tr><td>Primary Group Champion</td><td>Family Group Champaign</td></tr>
<tr><td>  </td><td>  </td></tr>
<tr><td>Secondary Group Champion</td><td>Open Group Champaion</td></tr>
<tr><td>  </td><td>  </td></tr>
</table>

Figure 6. Champion entries of Primary School, Secondary School, Open and Family Categories

Use this link to access the winning entries online:
https://www.cybersecurity.hk/en/contest-2019.php

We co-organised the 2-day Information Security Summit 2019 with other information security organisations and associations in October 2019, 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 2019 to promote the public seminar and the Poster Design Contest.

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 Singapore
- Participated in the FIRST Meeting and Conference, and the National CSIRT Meeting in Edinburgh, UK
- Participated in the CNCERT Conference in Guangzhou
- Participated in the HITCON Security Conference in Taipei
- 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". As of December 2019, over 150 Information Security companies and critical infrastructure organisations had joined the platform. Cyber security information and intelligence were shared among the members. HKCERT joined as a member of the Programme and shared security intelligence with the members. Through the platform, HKCERT also shared security alerts with the public. 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 collaborated with Microsoft in the Healthcare Cyber Security Watch Programme to promote cyber security situational awareness in healthcare

sector. The objective of this programme is to make use of global cyber threat intelligence to inform Hong Kong Healthcare sector of attacks targeting their IT infrastructure so that they can better mitigate security risks. The Programme was officially launched in December 2019 with 11 organisations including the Hospital Authority and most of the private hospitals in Hong Kong joining.

5. Other Achievements

5.1 Strategy and Service Review

HKCERT had conducted a Strategy and Service Review by external reviewer in October 2019. The preliminary findings were received by HKCERT and OGCIO Hong Kong SAR Government in January 2020.

5.2 Advisory Group Meeting

HKCERT had held the Advisory Group Meeting in October 2019. The meeting solicited inputs from the advisors on the development strategy of HKCERT.

5.3 Three Year Strategic Plan

HKCERT prepared its rolling Three Year Strategic Plan based on inputs from Advisory Group, the Strategy and Service Review Report and discussion with the government. The plan would be updated annually. HKCERT based on this plan to prepare the annual work 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.

5.5 IoT Security Study and Best Practice

HKCERT placed more efforts in IoT Security. We joined the APCERT IoT Security Working Group. In 2019 HKCERT released an IoT Device (Webcam) Security Study. In Q1 of 2020, HKCERT planned to release the IoT Security Best Practice and three other studies in IoT network protocols.

5.6 Open Data

HKCERT had a plan to provide open data for the count of monthly security incidents on website for public access (see https://www.hkcert.org/open-data) starting January 2020.

5.7 Year Ender press briefing

HKCERT organised a year ender press briefing to media in January 2020 to review cyber security landscape of 2019 and provided an outlook to 2020 to warn the public for better awareness and preparedness. It received very good press coverage.

Security Outlook for 2020
2020年的資訊保安展望

1. New Technologies Bring New Exposure
   新科技帶來新威脅
2. Cyber Attacks More Targeted and Organised
   網絡攻擊變得更具針對性和有組織
3. Security Issues from the End of Support (EOS) to Technologies
   因支援服務終止（EOS）引起的網絡保安問題
4. Supply Chain Attacks Bypass Enterprise Defence
   供應鏈攻擊繞過企業的保安系統
5. Mobile Payment Services Being Targeted
   流動支付服務成為攻擊目標
6. Data Breaches Reports and Penalties on the Rise
   數據外洩報告和處罰上升

Figure 7. 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 2020/2021. 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

In the coming year, HKCERT will invest on more digital campaign for security awareness promotion. HKCERT will collect inputs from incident reporters via survey. HKCERT will re-design and revamp its website to replace the old design to enhance user experience and engagement.

7. Conclusion

HKCERT recorded significant hikes in botnet and phishing website reports in Hong Kong for 2019. In 2020, the wider use of new technologies such as IT/OT, AI deepfake and 5G are expected to contribute to bring about new cyber security challenges. HKCERT will continue to put effort in IoT security and advise enterprises to adopt a “Security by Design” approach to manage cyber risk.

Moreover, computers running an older version of Microsoft operating systems and Transport Layer Security (TLS) protocols will face more security threats with the end of official technical support and security patch. HKCERT will urge enterprises to plan upgrade/migration for end of support operating systems and protocols and implement them when required.

-- END --