ANNUAL REPORT 2020

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 2020

1. Highlights of 2020

1.1 Summary of Major Activities

- Organised the "Build a Secure Cyberspace 2020" campaign with the Government and Hong Kong Police Force. The campaign involved public seminars, and a Mobile Sticker Design Contest.
- Organised the first "Hong Kong Cyber Security New Generation Capture the Flag Challenge 2020". It involved a 48-hours online contest and a public seminar with award ceremony.
- Presented in different international conferences and local press briefing.
    - "Introduction of HKCERT IoT Security Best Practice" in NatCSIRT Conference.
    - "Performing IoT Security Testing" in APCERT Training Workshop.
    - "Cyber Security Status of SMEs in HK" in 2020 APEC SME Cyber Security Forum.
    - "Year Ender" in local medias briefing.
- Published timely security guidelines and advisories in response to the digital transformation during the COVID-19 pandemic period.

1.2 Achievements & Milestones

- Conducted a strategy and service review by external assessor. Findings and improvement areas are shared in the advisory group meeting and incorporated in the strategic plan.
- Revamp the official website for better support of mobile users and improving user experience.
- Produced animation videos and leveraged social media platform to promote cyber security awareness to general public.
- Published IoT Security Study and Best Practices for local enterprises and IoT developers.
- Launched HKCERT LinkedIn Page to target for different user groups.

2. About HKCERT

2.1 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.

2.2 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.

2.3 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 defence 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

3. Activities and Operations

3.1 Incident Handling

During the period from January to December of 2020, HKCERT had handled 8,346 security incidents which was 12% decrease of the previous year (see Figure 1). Referral cases accounted for 95% of the total number of security incidents.

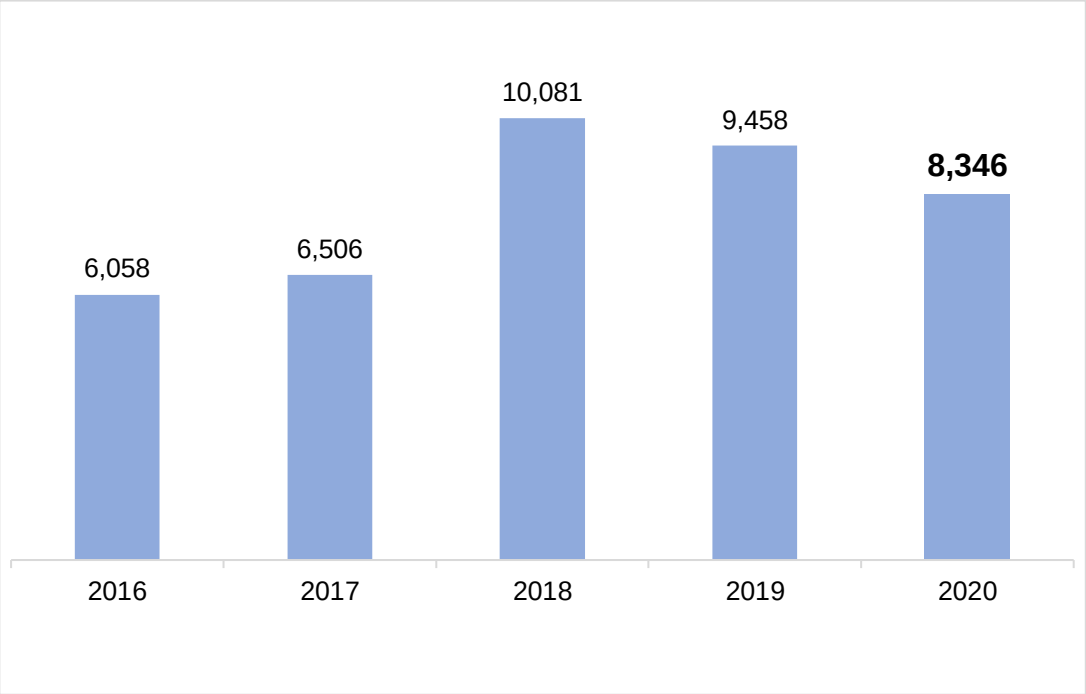


Figure 1. HKCERT Security Incident Reports

While the number of overall security incidents handled by HKCERT reported a drop for the second year running, falling 12% year-on-year to 8,346 in 2020. Phishing (3,483 cases or 42%) went up 35% with cyber criminals exploiting the surge of online activities due to the pandemic. On the other hand, botnets (4,154 cases or 50%), remaining the top source of reported incidents, and malware (181 cases or 2%) fell 16% and 85% respectively. The drop of malware cases was due to more malware targeting enterprises for higher return and the number of individual based reports significantly dropped (see Figure 2).

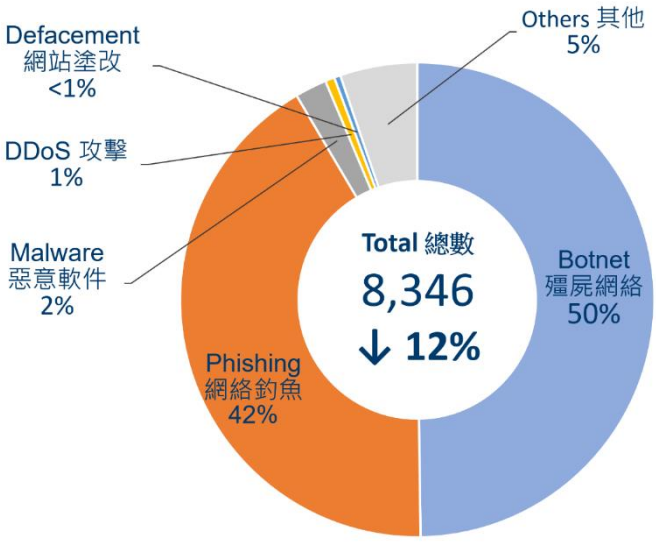


Figure 2. Distribution of Incident Reports in 2020

3.2 Watch and Warning

During the period from January to December of 2020, HKCERT published 315 security bulletins (see Figure 3) on the website. In addition, HKCERT have also published 43 blogs, including security advisories on home office, online conferencing tools, personal VPN service, enterprise VPN security, DDoS extortion attacks, ransomware trends, TLS version upgrade, etc.

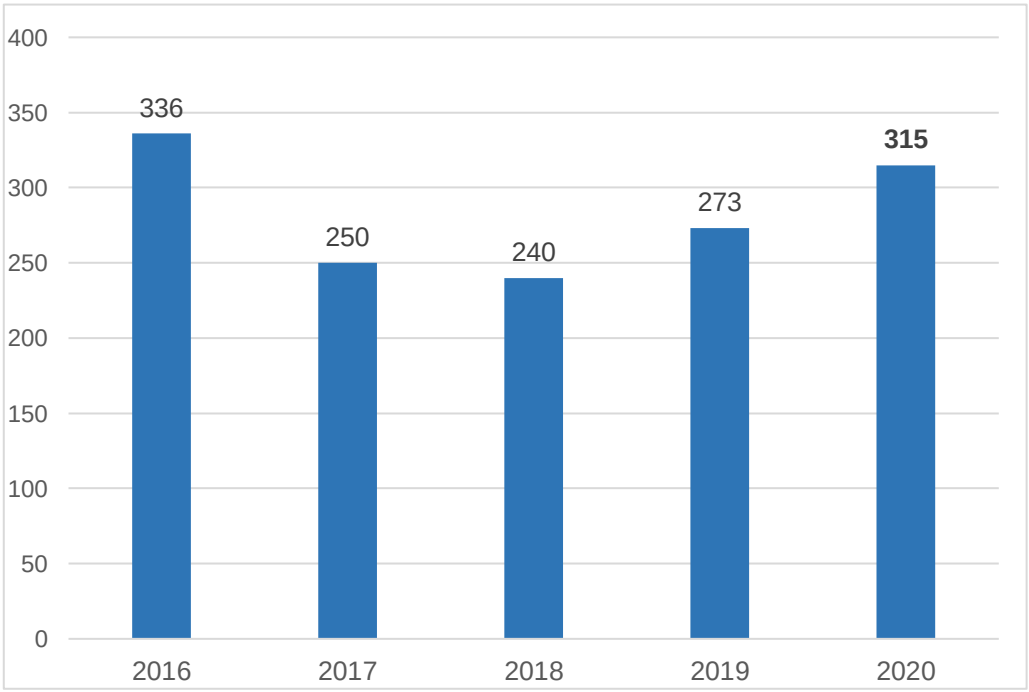


Figure 3. HKCERT Published Security Bulletins

The drop of Security Bulletins in 2017 was mainly due to consolidation of MS & Adobe security bulletins

HKCERT used the centre's website (https://www.hkcert.org), RSS, Hong Kong Government Notification mobile app, social media platforms such as Facebook and LinkedIn 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.

3.2.1 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 high count of 8,017 in 2020 Q1 and dropped gradually to 4,372 in Q4 2020, largely attributed to the Mirai botnet events as depicted in Figure 5.

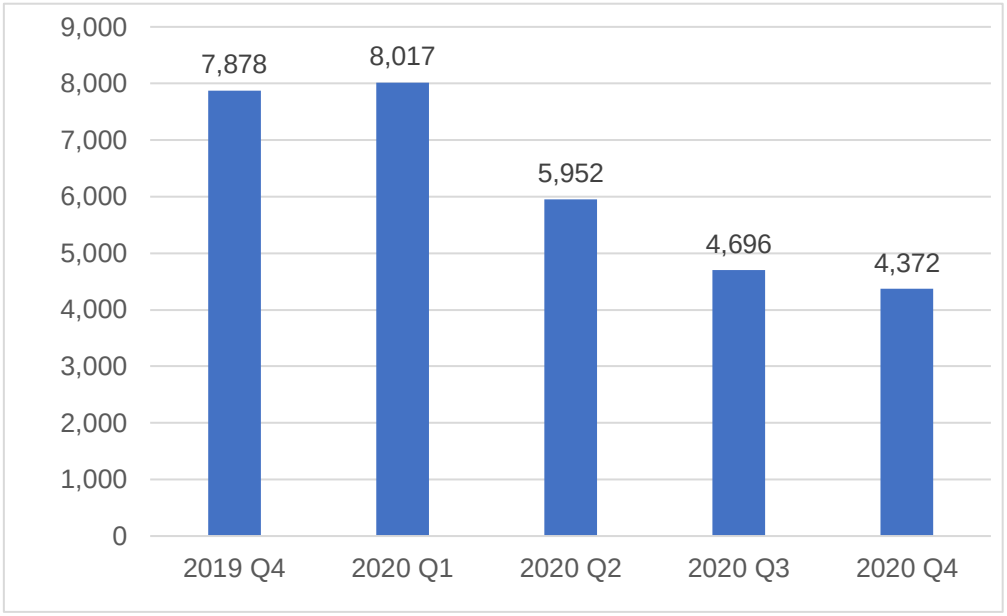


Figure 4. Trend of Bot related security events in the past year
(Source: data feeds from overseas security researchers, not from incident reports)

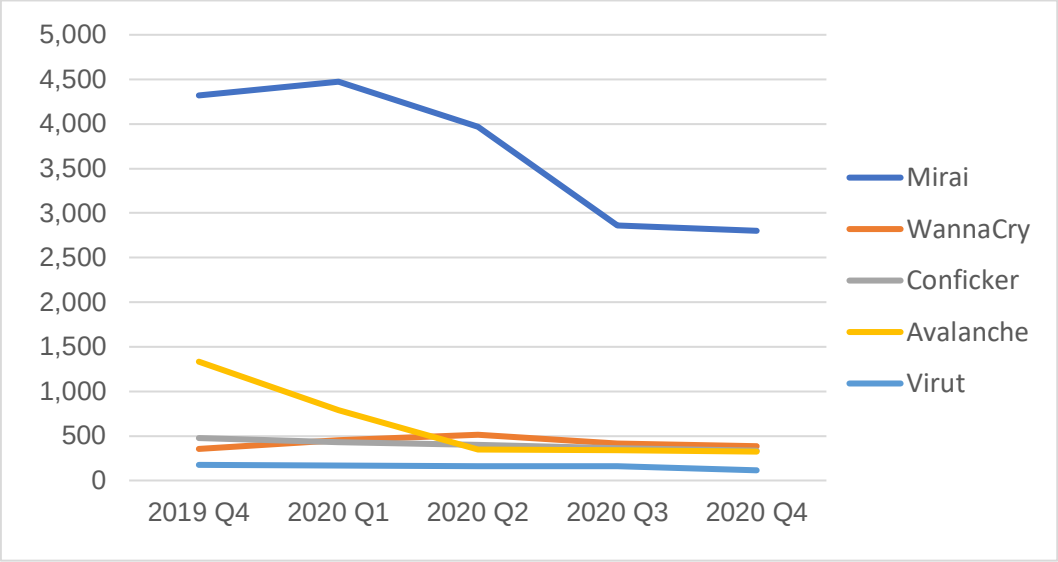


Figure 5. Trend of Top 5 Botnet Families in the past year

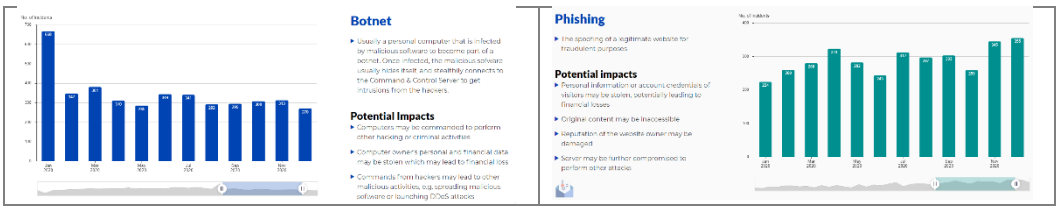
(Source: data feeds from overseas security researchers, not from incident reports)

3.3 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 every quarter (see Figure 6) (see https://www.hkcert.org/statistics).



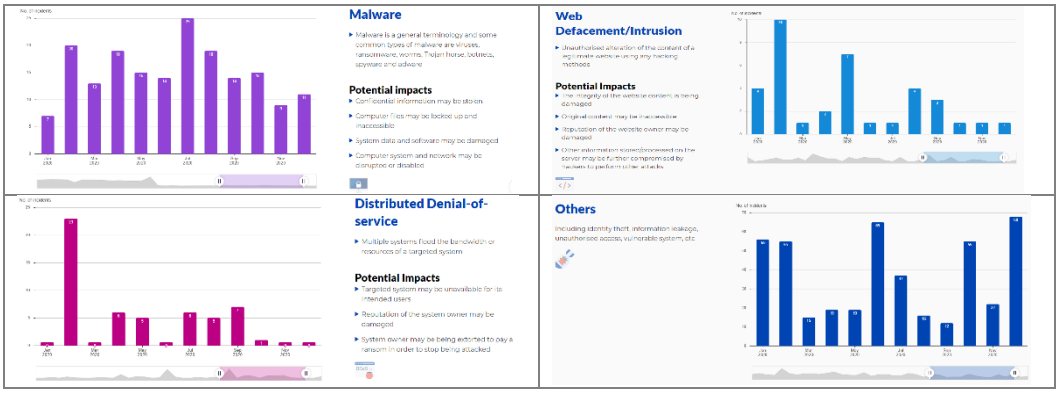


Figure 6. Charts in HKCERT website showing the statistics of different types of incident reports.

4. Events organised and co-organised

4.1 Seminars, Conference and Meetings

HKCERT jointly organised the “Build a Secure Cyberspace 2020” campaign with the Government and Hong Kong Police Force. The campaign involved public seminars, and a Mobile Sticker Design Contest. A public seminar was organised in May 2020. For the Poster Design Contest, HKCERT 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 7).

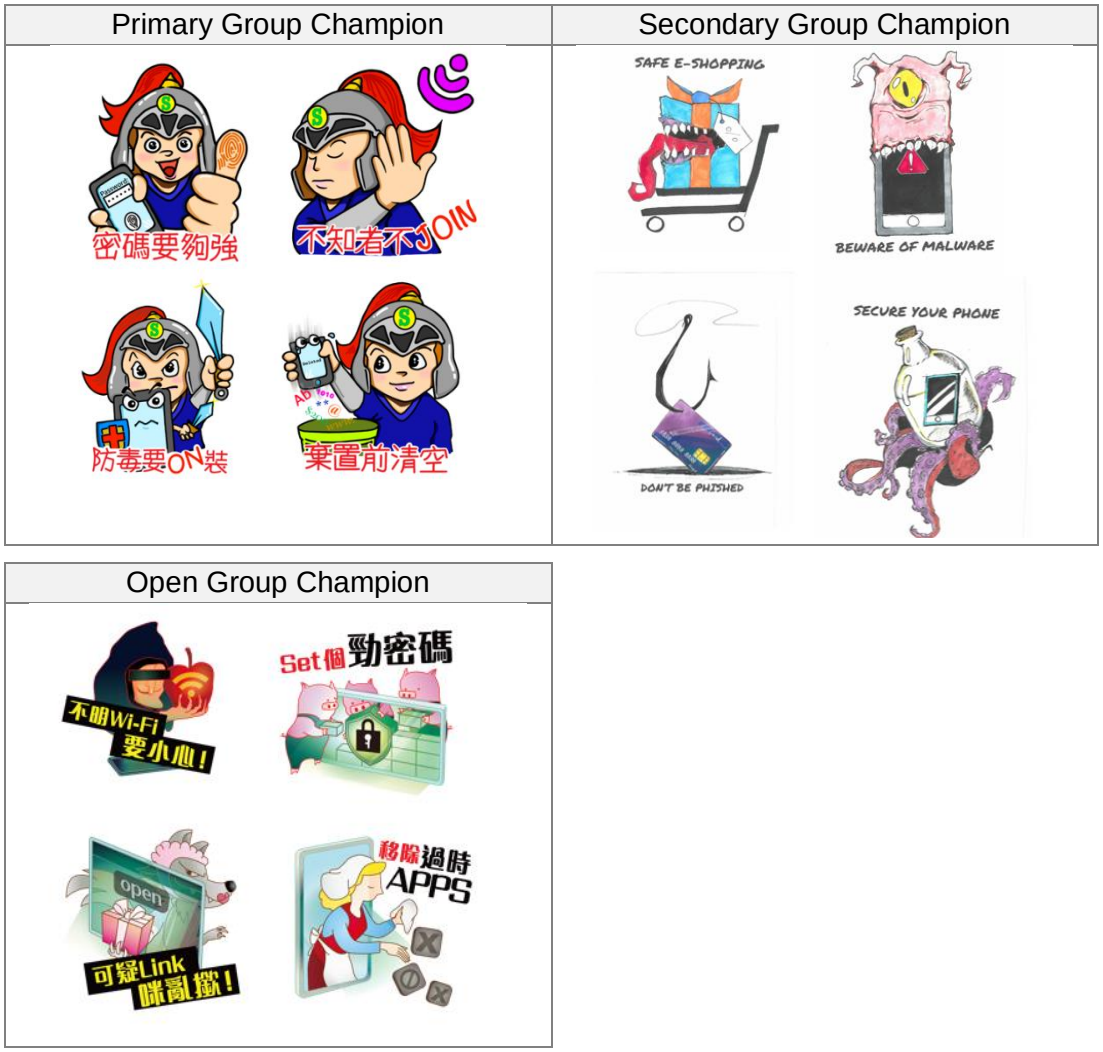


Figure 7. Champion entries of Primary School, Secondary School, Open and Family Categories

Use this link to access the winning entries online:
https://www.cybersecurity.hk/en/contest-2020.php

4.2 Capture The Flag Contest

HKCERT jointly organised the "Hong Kong Cyber Security New Generation Capture the Flag Challenge 2020" with partner associations in information and education sectors. The 48-hours contest was opened to secondary and tertiary institutions. It was a success with 156 teams and 541 students participating. A public seminar with award ceremony was organised in November 2020.

Use this link to access the webinar playback and winning entries online:

- https://www.hkcert.org/event/hong-kong-cyber-security-new-generation-capture-the-flag-challenge-2020-webinar-and-award-presentation-ceremony
- https://www.hkcert.org/press-center/the-capture-the-flag-challenge-2020-award-presentation-ceremony-recognises-cyber-security-future-talents

4.3 Speeches and Presentations

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

4.4 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.

4.5 Media Promotion, Briefings and Responses

HKCERT invited 4 media agencies for a roundtable sharing on the summary of first half year of 2020 based on Hong Kong Security Watch Report. During the session, HKCERT also shared the cyber security posture and security advices in the New Normal era.

5. Collaboration

5.1 International Collaboration

HKCERT participated in a number of international coordination and collaboration events in year 2020:

- Delivered “Introduction of HKCERT IoT Security Best Practice” presentation in NatCSIRT Conference
- Delivered “Performing IoT Security Testing” in APCERT Training Workshop
- Delivered “Cyber Security Status of SMEs in HK” presentation in 2020 APEC SME Cyber Security Forum
- Participated in the APCERT AGM and Web Conference
- Participated in the FIRST AGM and Web Conference
- Participated in CNCERT Annual Web Conference
- Participated in the HITCON Annual Web Conference
- Participated in the AusCERT Annual Web Conference
- Participated in (ISC)2 APAC Security Congress
- Participated in APCERT Drill and OIC-CERT Cyber Security Drill Exercise

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

5.2 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.
- HKCERT continued to actively participate in the Cyber Security Information Sharing platform ‘Cybersec Infohub” which comprised of over 300 companies, critical infrastructure organisations, banks and other enterprises in Hong Kong.
- 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 2020 with 12 organisations including the Hospital Authority and most of the private hospitals in Hong Kong joining.

6. Achievements & Milestones

6.1 Strategy and Service Review

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

6.2 Advisory Group Meeting

HKCERT had held the Advisory Group Meeting in October 2020. The meeting solicited inputs from the advisors on the development strategy of HKCERT.

6.3 Three Year Strategic Plan

HKCERT had 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 is updated annually. HKCERT based on this plan to prepare the annual work plan and budget to solicit funding support from the government.

6.4 HKCERT Website Revamp

HKCERT had revamped the official website (https://www.hkcert.org) in Dec 2020. The new website is enhanced with modern look and feel. It brings several benefits to users including: (1) adopted responsive design which provides greater support for mobile users; (2) enhanced the search function with better result relevance; (3) customisable RSS subscription (4) provided interactive chart for incident report statistic.

6.5 Cyber Security Awareness Video Campaign

HKCERT had produced a series of cyber security animation videos and leveraged social media to promote to local public. The aim was to raise their cyber security awareness. The series had 4 episodes using the theme “Hack me if you can”. The first episode about the security tips for remote work and video conferencing software was published in Dec 2020. The other 3 episodes will be published by Mar 2021.

Remote Work and Web Meeting Security Tips

https://youtu.be/FH7zWAb4-GQ

6.6 IoT Security Study and Best Practice

HKCERT placed more efforts in IoT Security. HKCERT joined the APCERT IoT Security Working Group. Further to the IoT Device (Webcam) Security Study released in 2019, in Q1 of 2020, HKCERT released the IoT Security Best Practice and several studies in IoT wireless network protocols: ZigBee, Wi-Fi and Bluetooth.

6.7 Security Guidelines and Advisories for the COVID-19 Pandemic

HKCERT published different security guidelines and alerts in response to the digital transformation during the COVID-19 pandemic period, such as guidelines for enterprise and personal VPN, remote access services, online meetings, security tips for home office and advisories on COVID-19 themed attacks.

6.8 HKCERT LinkedIn Page

HKCERT launched its LinkedIn page to target for different types of local Internet users and increase visibility.

6.9 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.

6.10 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.

6.11 Year Ender Press Briefing

HKCERT organised a year ender press briefing to media in January 2021 to review cyber security landscape of 2020 and provided an outlook to 2021 to warn the public for better awareness and preparedness. It received very good press coverage.

Figure 8. HKCERT at the Year Ender press briefing.

7. Future Plans

7.1 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.

7.2 Funding

HKCERT had secured Government funding to provide the basic CERT services in 2021/2022. We shall work closely with the Government to plan for the future services of HKCERT and seek their support.

7.3 Enhancement Areas

In the coming year, with the success of the first Capture The Flag (CTF) contest, HKCERT will continue to partner with different associations to organise another CTF in 2021. Beside the local secondary school and tertiary institution groups, HKCERT will also add the open group contest.

HKCERT will enhance internal incident reporting systems to automate the response and handling process. HKCERT will partner with different security organsiations or companies to provide situational threat intelligence information to the general public in order to raise the awareness and improve the cyber hygiene.

8. Conclusion

In 2020, the number of overall security incidents reported to HKCERT recorded a drop for the second year running. Phishing increased by 35% with cyber criminals exploiting the surge of online activities amid pandemics. On the other hand, botnet and malware fell 16% and 85% respectively. The latter was due to a drop of massive individual ransomware cases as cyber criminals moved to target enterprises for higher monetary return.

In 2021, HKCERT urges enterprises to quickly put in place cyber security strategy for the new normal and new technologies, in order to combat an anticipated surge in cyber attacks arising from accelerated digital transformation amid the pandemics and the use of emerging technologies such as 5G communication, Internet of Thing (IoT) and AI. Furthermore, HKCERT also urges enterprises to be ready for an escalation in supply chain attacks in which attackers leverage on the trust of an enterprise on its supply chain partners to bypass traditional defences. HKCERT will also promote cloud security and groom the next generation cyber security talents.

-- END --