ANNUAL REPORT 2022

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 2022

1. Highlights of 2022

1.1 Summary of Major Activities

- Organised the "Build a Secure Cyberspace 2022" campaign with the Government and Hong Kong Police Force.
- Organised the "Hong Kong Cyber Security New Generation Capture the Flag Challenge 2022".
- Published an Incident Response (IR) Guideline and a one-page infographic for the guideline.
- Organised the "Small and Medium Enterprise (SME) Cyber Security Connection Programme".
- Launched the Open Threat Intelligence Campiagn
- Presented in different international conferences and local press briefing.
    - "Year Ender" in local media briefing to call on public to raise awareness of information security
    - Media interviews in local media, radio and TV programme to raise general public awareness on cyber security risks.
- Published timely security guidelines and advisories in response to the digital transformation.

1.2 Achievements & Milestones

- Organised the "Build a Secure Cyberspace 2022" campaign with the Government and Hong Kong Police Force. The campaign involved 2 public webinars, a Folder Design Contest and an award presentation ceremony. Over 1,000 participants joined the contest and over 1,200 participants joined the 2 webinars.
- Organised "Hong Kong Cyber Security New Generation Capture the Flag Challenge 2022". It involved 3 workshops, a 48-hours online contest and a public webinar with award ceremony. 434 teams and more than 1100 participants from universities, secondary schools and security practitioners joined the contest. The contest was the second time expanded to have open group category and international teams invited.
- Published the "Incident Response Guideline for SMEs" and a one-page infographic for the guideline to guide organisations how to deal with common cyber

attacks

- Published security advisories on latest phishing and ransomware attacks patterns and emerging cyber threats
- Collaborate with Cybersec infohub to launch the Open Threat Intelligence Campaign and provide automatic integration of threat intelligence feeds by means of machine-to-machine (M2M) sharing
- Continued the Healthcare Cyber Security Programme and Critical Infrastructure Cyber Security Programme. The which covered almost all public and private hospitals of Hong Kong.
- Launched the SME Cyber Security Connection Programme, which engaged 11 organisations from different sectors of SMEs in Hong Kong and organized 9 webinars .The topics of webinars covered the latest cyber security threats and the guideline for incident response.

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 2022, HKCERT had handled 8,393 security incidents which was 9% increase of the previous year (see Figure 1).

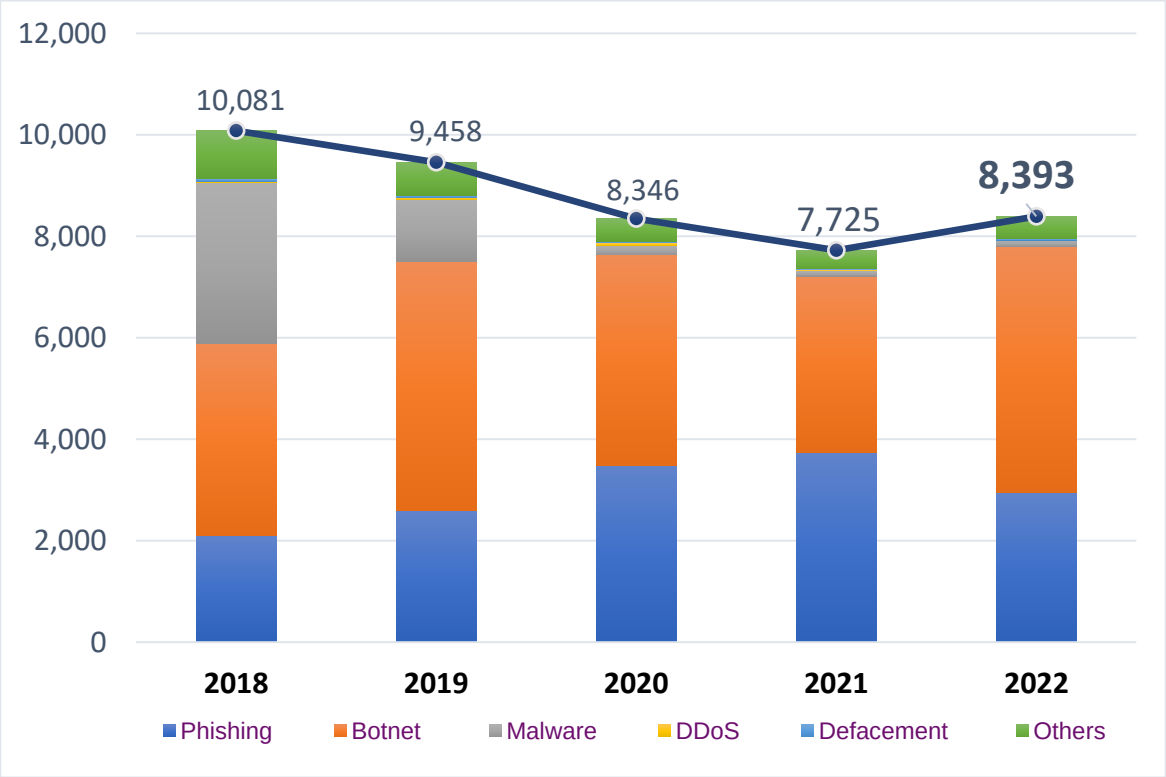


Figure 1. HKCERT Security Incident Reports

While the number of overall security incidents handled by HKCERT reported a rise after three consecutive years of decline since 2018, increasing 9% year-on-year to 8,393 in 2022. Phishing (2,946 cases or 36%) went down 21% but total phishing URLs was increased by 4%. On the other hand, botnets (4,858 cases or 58%), remaining the top source of reported incidents increased 40%. The increase of botnet cases was partly due to cybercriminals abusing a red-team kit, Cobalt Strike, to launch sophisticated attacks.

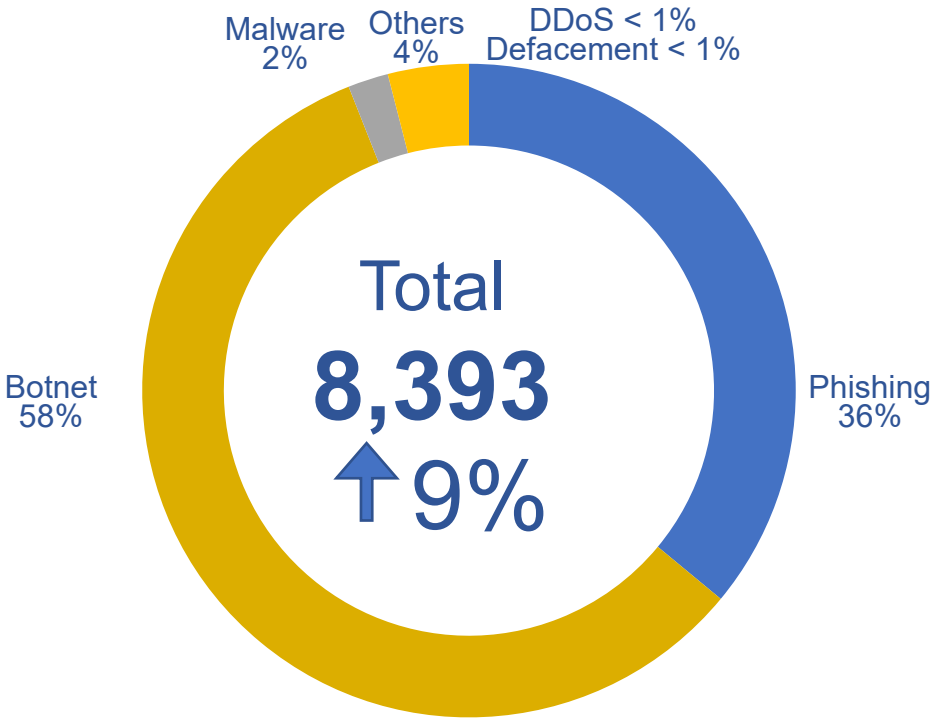


Figure 2. Distribution of Incident Reports

3.2 Watch and Warning

During the period from January to December of 2022, HKCERT published 350 security bulletins for the vulnerabilities of major software (see Figure 3) on the website. In addition, HKCERT have also published 35 security advisories, topics include zero trust architecture, analysis of malware and browser's anti-phishing feature, incident response guideline for SME, security risk of emerging technologies such as NFT, QR Code, artificial intelligence, etc.

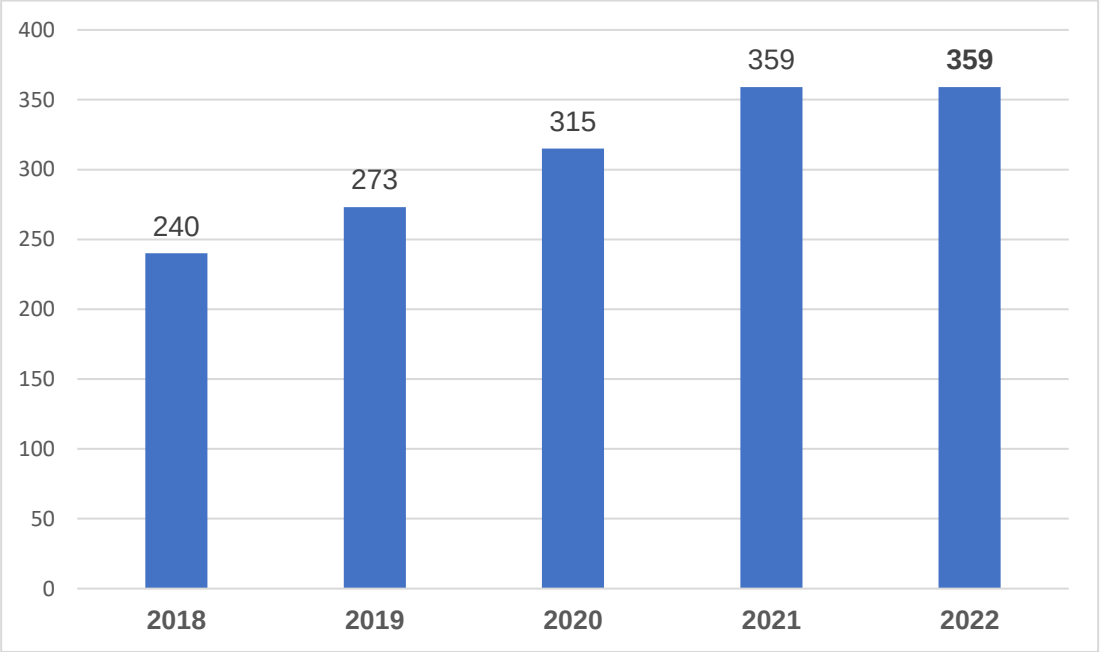


Figure 3. HKCERT Published Security Bulletins

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 3,684 in 2022 Q3. The major botnet remained as Mirai.

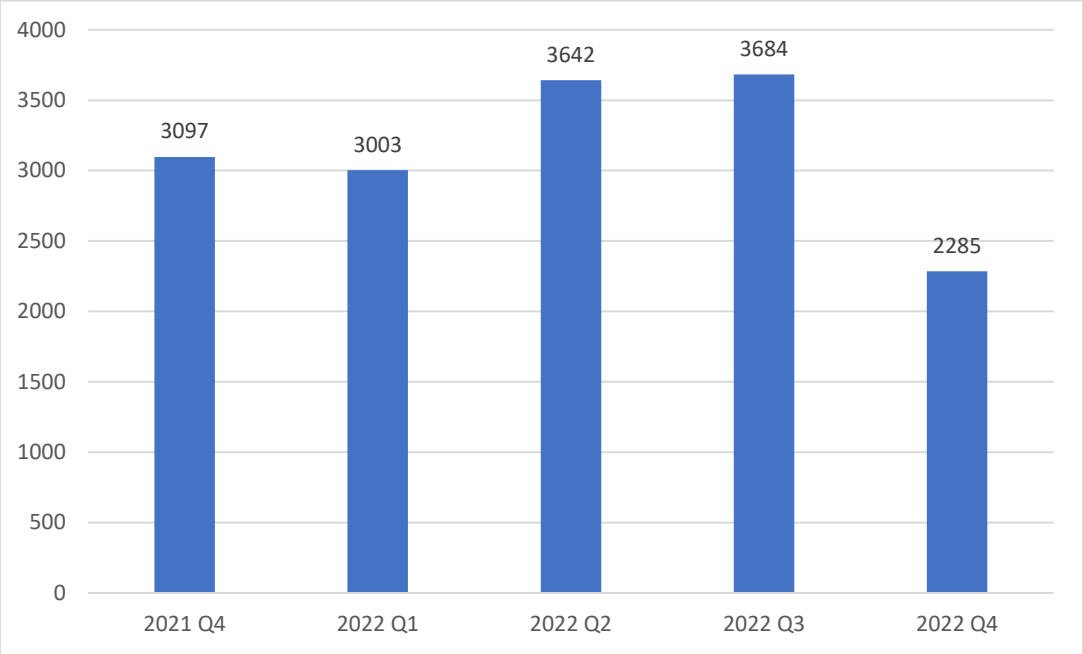


Figure 4. Trend of Bot related security events in the past year
(Source: data feeds from overseas security researchers, not from incident reports)

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/watch-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 every quarter (see Figure 5) (see https://www.hkcert.org/statistics).

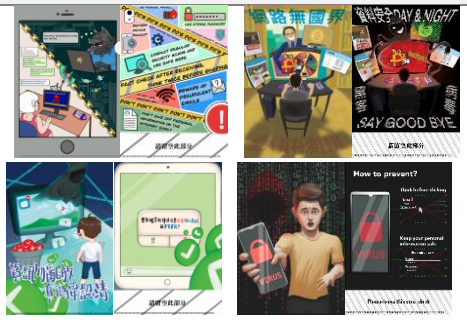
Figure 5. Charts in HKCERT website showing the statistics of different types of incident reports.

4. Events organised and co-organised

4.1 Build a Secure Cyberspace 2022

HKCERT jointly organised the “Build a Secure Cyberspace 2022” campaign with the Government and Hong Kong Police Force. The campaign involved 2 public webinars, and a Folder Design Contest. An award presentation ceremony was organised in Sep 2022.

For the Folder Design Contest, HKCERT received about more than 1,000 applications from Open Group, Secondary School and Primary School Group. A professional judge panel selected winners with most creative and outstanding design (see Figure 6).

Primary Group Champion	Secondary Group Champion
	

Open Group Champion

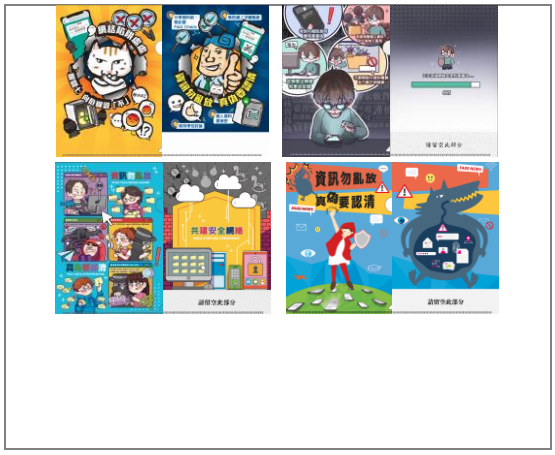


Figure 6. Champion entries of Primary School, Secondary School, Open Categories

Use this link to access the winning entries online:
https://www.cybersecurity.hk/en/contest-2022.php

4.2 Capture The Flag Contest

HKCERT jointly organised the "Hong Kong Cyber Security New Generation Capture the Flag Challenge 2022" with partner associations in information and education sectors. The 48-hours contest was opened to secondary and tertiary institutions. It was a success with 434 teams and more than 1,100 participants from universities, secondary schools and open categories. This year we also invited 10 teams from overseas countries to compete with local participants. A public webinar with award ceremony was organised in December 2022.

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-2022-webinar-and-award-ceremony

4.3 Small and Medium Enterprise (SME) Cyber Security Connection Programme

HKCERT launched the SME Cyber Security Connection Programme to raise the security awareness of SMEs in Hong Kong, 11 SMEs associations were engaged and 9 webinars were delivered. Topics included the latest cyber security threats and incident response guideline. A discussion session was held to understand the pain point of SMEs on cyber security and explained the services of HKCERT to support their cyber security effort

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. banks, government, retail, manufacturing, SMEs, education, etc.

4.5 Media Promotion, Briefings and Responses

HKCERT attended several media interviews from local media, radio and TV programme to share the cyber security issues and provide security advices on user awareness, phishing, online scam and emerging technologies such as metaverse and NFT. HKCERT issued media messages for security hot topics and generated more than 200 reports of media coverage.

5. Collaboration

5.1 International Collaboration

HKCERT participated in a number of international coordination and collaboration events in year 2022:

- Participated in the NatCSIRT Conference 2022 and presented “HK SME Cyber Security Connection Programme”
- Participated in the OIC-CERT Webinar 2022 and presented “Raise Cyber Security Awareness and Capacity in HK”
- Participated in the HITCON 2022 (Online)
- Participated in the 2022 APCERT Cyber Security Drill Exercise

- Participated in the APCERT AGM and Conference 2022
  - Presented “Safeguarding IoT Devices in Digital Age – How HKCERT Adds Values to the Industries”
- CNCERT International Partnership Conference
  - Presented “Safeguarding IoT Devices in Digital Age – How CERT can Improve Cyber Readiness”

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 14 organisations including the Hospital Authority and most of the private hospitals in Hong Kong joining.
- HKCERT collaborated with Microsoft in the Critical Infrastructure Cyber Security Watch Programme to promote cyber security situational awareness in critical infrastructure sector. The objective of this programme is to make use of global cyber threat intelligence to inform Hong Kong critical infrastructure sector of attacks targeting their IT infrastructure so that they can better mitigate security risks. The Programme was officially launched in December 2021 with 7 organisations that provide essential public services to the citizens in Hong Kong joining.

- HKCERT collaborated with local regulators to deliver talks to related regulated organisations and members.
- HKCERT collaborated with local universities to conduct research on IoT and OT security.

6. Achievements & Milestones

6.1 Advisory Group Meeting

HKCERT had held the Advisory Group Meeting in September 2022. The meeting solicited inputs from the advisors and invited guests from SME associations on the development strategy of HKCERT.

6.2 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.

6.3 HKCERT Incident Response Guideline for SMEs

HKCERT had launched the "Incident Response Guideline for SMEs" (https://www.hkcert.org/security-guideline/incident-response-guideline-for-smes) in Jul 2022. The guideline covered information of 3 areas to aid user to handle cyber attacks. These 3 areas include (1) Maintain and maximise their systems' defences with limited resources, (2) Minimise business and financial impacts in cyber incidents, and (3) Prevent and minimise the reoccurrence of similar cyber attacks

6.4 HKCERT "Open Threat Intelligence Campaign

HKCERT had launched the Open Threat Intelligence Campaign and used Cybersec infohub as an integrated intelligence sharing platform to provide automatic integration of threat intelligence feeds with organisations' security systems by means of machine-to-machine (M2M) sharing. The objective is to help organisations enhancing their cyber security defence capabilities by leveraging HKCERT threat intelligence for early identification or proactive blocking of suspicious network activities.

6.5 Analysis of Latest Malware Behavior

HKCERT studied and analysed the infection vector and malicious behavior of the 2 malware: QBot and AgentTesla. Advisories were published to raise situational awareness of users for the prevention and detection measures.

6.6 Security Guidelines and Advisories for Emerging Cyber Threats

HKCERT published different security guidelines and alerts in response to the

emerging cyber threats and incidents happened in other regions, such as vulnerabilities in Apple, Microsoft, remote access device and storage device, protection of sensitive information in social media, NFT, AI, etc.

6.7 Analysis of Browser's Anti-phishing Feature

HKCERT studied and analysed the performance of anti-phishing feature of common browsers. The objective is to allow users understand the limitation of technology and emphasis the importance of security awareness against phishing.

6.8 Research on IoT and OT security

HKCERT collaborated with local universities to conduct researches on the security of drone and operation technology. The researches were successful and HKCERT published a video of drone hacking to raise the security awareness of IoT device.

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 February 2023 to review cyber security landscape of 2022 and provided an outlook to 2023 to warn the public for better awareness and preparedness. It received very good press coverage.

Figure 7. 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 2023/2024. 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 increasing trend of phishing attack, HKCERT will launch the "Be Smart, Spot the Phish" campaign. It involves a roving exhibition through booth and vehicle to different regions of Hong Kong and explains how to tackle phishing attack to the citizens of Hong Kong. Also a themed web page about phishing with preventive measure and latest phishing samples for raising the situational awareness will also be launched as part of the campaign.

HKCERT will continue to organise the Capture The Flag (CTF) contest, HKCERT will continue to partner with different associations to organise another CTF in 2023 for the participants from universities, secondary schools and open categories.

8. Conclusion

In 2022, the number of overall security incidents reported to HKCERT recorded a rise (9%). Phishing URLs increased by 4% with cyber criminals exploiting the surge of online activities amid pandemics. Botnet also recorded an increase (40%). The increase of botnet cases would be due to cybercriminals abusing to use a red-team kit, Cobalt Strike

In 2023, HKCERT will continue to actively study the trends of cyber attacks and security technologies, and assist the community in meeting the ever-changing security challenges through various channels, such as issuing early warnings of cyber attacks, security recommendations, etc. HKCERT will also organise major international seminars and competitions, including the Information Security Summit and the Hong Kong Cyber Security New Generation Capture the Flag Challenge, to raise local cyber security awareness and nurture the next generation of cyber security talents.

There are five major information security risks that must be addressed in 2023:

1. Phishing attacks for identity or credential theft: In 2022, phishing attacks were consistently ranked among the top security incidents handled by HKCERT. Credential phishing is a common first step in identity theft by hackers to obtain sensitive personal information from users. Hackers are also using new techniques to bypass multiple authentication security measures.
2. Attacks using artificial intelligence (AI): AI systems have a deeper and wider range of potential cyber security risks than traditional systems. For example, if multiple services use the same AI model, and the model is tampered with by an attack, all services using the model will be affected. Hackers can also use AI to create fake messages, such as images and sounds, to blackmail, create pornographic videos, spread rumours and even bypass biometric authentication to steal people's identities.
3. The low cost of cybercrime services will attract more criminals: as the business model for cybercrime changes, cyber attacks have evolved into a service format, significantly lowering the hurdles to launch an attack. Cybercrime services can be very inexpensive, for example, you can buy 1,000 stolen accounts for less than US$1.
4. Web 3.0: The core concept is “decentralisation”, the most familiar application of

which is cryptocurrency and metaverse. 12% of phishing links handled by HKCERT in 2022 involved cryptocurrency. The Hong Kong Monetary Authority has brought virtual currency exchanges under regulation and required virtual asset service providers to obtain a licence on 1 June 2023, demonstrating that the security risks of Web 3.0 cannot be ignored.

5. Widespread application of IoT creates more opportunities for attacks: digitisation drives the development of "Industry 4.0", helping enterprises to improve their operational efficiency through smart manufacturing. “Industry 4.0” is one of the key elements of Hong Kong's new industrialisation, which integrates IT and operational technology (OT) systems and often applies different IoT devices to connect IT and OT systems to the Internet, increasing the number of entry and exit points or network interfaces, bringing new IS risks and threats.

-- END --