ANNUAL REPORT 2023

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 2023

1. Highlights of 2023

1.1 Summary of Major Activities

- Organised the "Build a Secure Cyberspace 2023" campaign with the Government and Hong Kong Police Force.
- Organised the "Hong Kong Cyber Security New Generation Capture the Flag Challenge 2023".
- Held "All-Out Anti-Phishing" moving showroom campaign.
- Participated in smart city roving exhibition organised by the Government.
- Participated in Innocarnival 2023 organised by Innovation and Technology Commission.
- 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 2023" campaign with the Government and Hong Kong Police Force. The campaign involved 2 public seminars , a Speech Contest and an award presentation ceremony. Over 150 participants joined the contest and over 400 participants joined the seminars.
- Organised "Hong Kong Cyber Security New Generation Capture the Flag Challenge 2023". It involved 2 workshops, a 48-hours online contest and a public seminar with award ceremony. The international category was the first time to open for registration and attracted over 100 teams to participate. HKCERT also collaborated with SECCON and could assign 1 winning team in tertiary or open categories to participate in SECCON CTF 2023 final.
- Held "All-Out Anti-Phishing" moving showroom campaign. It involved 3 phases and over 10 different locations in Hong Kong. HKCERT crossed over DinDong designer to design an anti-phishing themed moving showroom. The campaign

visited Hong Kong, Kowloon, and the New Territories to teach citizens how to identify and prevent phishing attacks.

- Participated in smart city roving exhibition organised by the Government. It involved how various smart city initiatives in Hong Kong can bring convenience to their daily life through the adoption of technology. HKCERT held a booth in the exhibition to raise the awareness of cyber security among the public.
- Participated in Innocarnival 2023 organised by Innovation and Technology Commission. HKCERT held a booth in the activity and interacted with the public via deepfake technology.
- Published security advisories on latest phishing and ransomware attacks patterns and emerging cyber threats
- Continued the Healthcare Cyber Security Programme and Critical Infrastructure Cyber Security Programme. The which covered almost all public and private hospitals of Hong Kong.

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 2023, HKCERT had handled 7,752 security incidents which was 8% decreased of the previous year (see Figure 1).

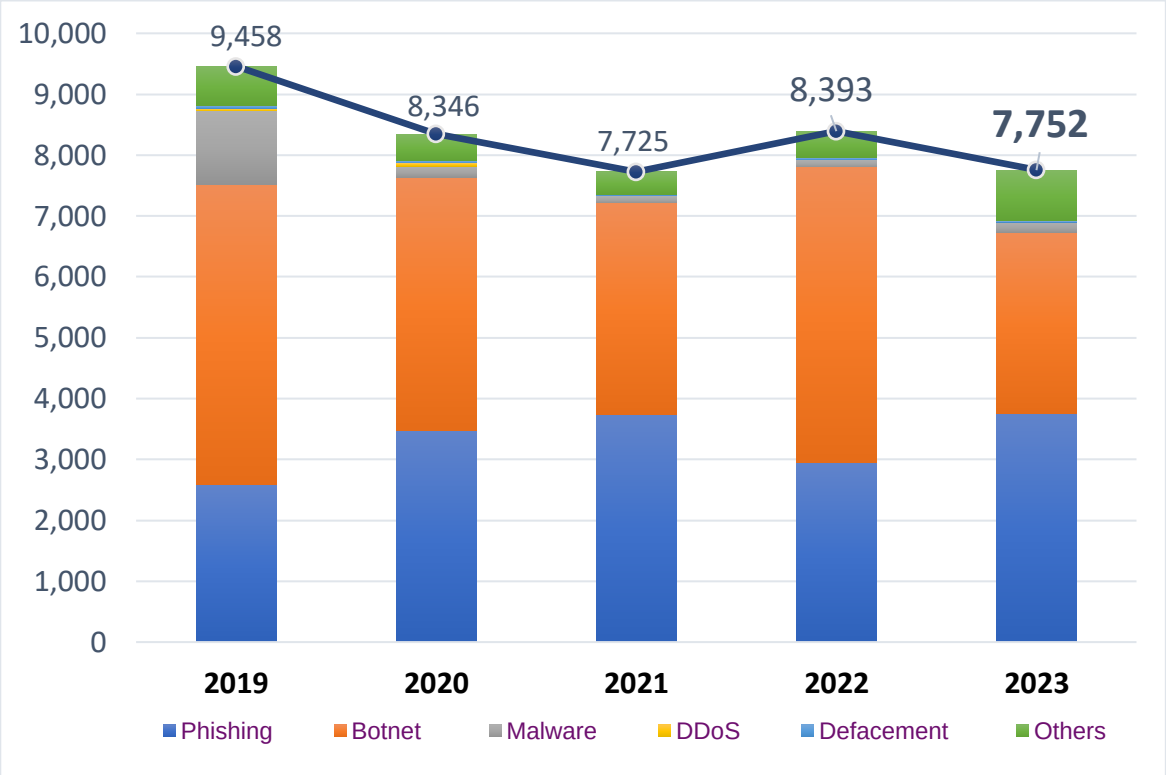


Figure 1. HKCERT Security Incident Reports

While the number of overall security incidents handled by HKCERT kept fluctuating since 2020. The amplitude ranged from -9% to +9%. Phishing (3,752 cases or 48% of total cases) went up 27% and total phishing URLs was increased by 22%. During the period from March to April of 2023, Hong Kong seriously suffered from phishing attacks targeting reward programs of some Hong Kong organisations. On the other hand, botnets (2,982 cases or 38% of total cases) dropped significantly and went down 39%.

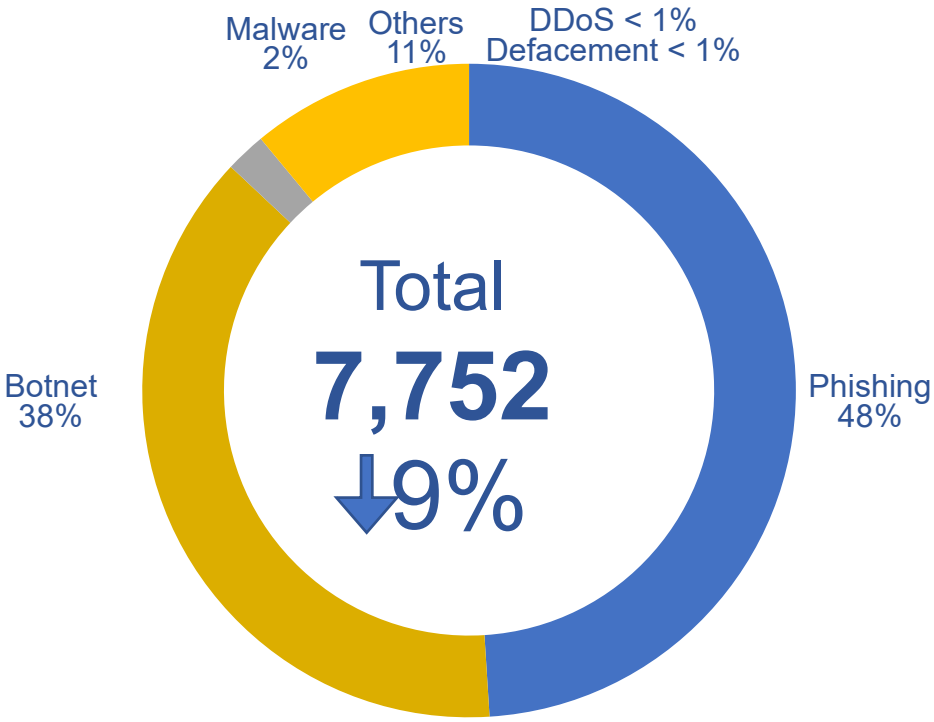


Figure 2. Distribution of Incident Reports

3.2 Watch and Warning

During the period from January to December of 2023, HKCERT published 357 security bulletins for the vulnerabilities of major software (see Figure 3) on the website. In addition, HKCERT have also published 31 security advisories, topics include 5 key risks in Hong Kong Information Security Outlook 2023 such as artificial intelligence, IoT, Crime-as-a-service, Web 3.0 and identity theft, analysis of ransomware trend across Asia-Pacific, guideline for using artificial intelligence and instant message application.

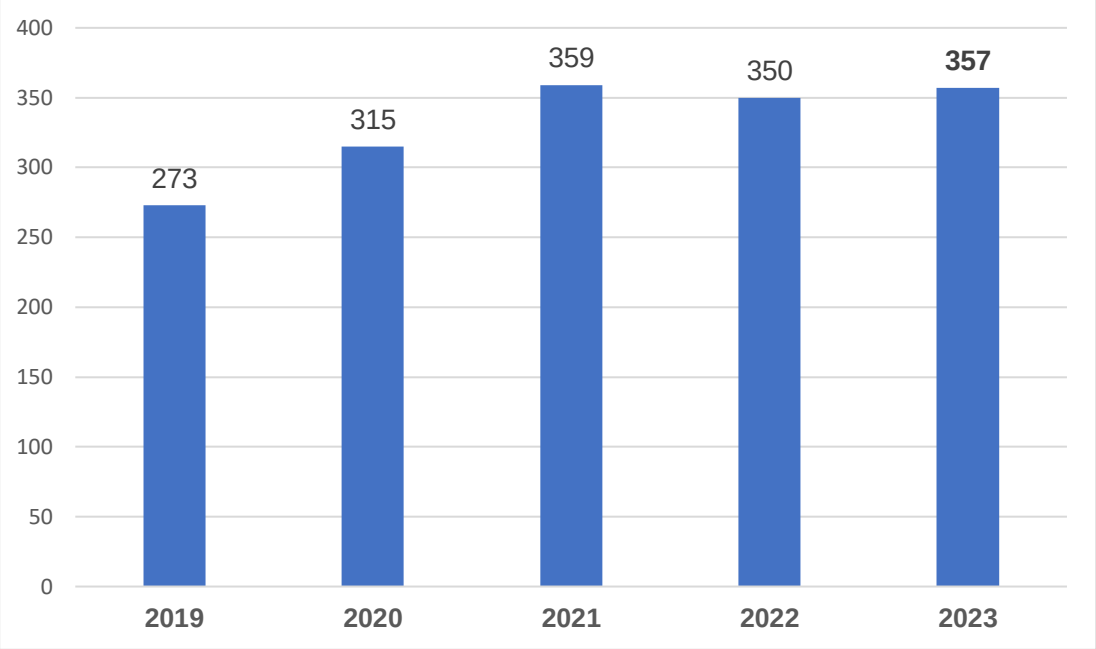


Figure 3. HKCERT Published Security Bulletins

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 2,583 in 2023 Q1 and kept up and down in subsequent quarters. The major botnet remained as

Mirai.

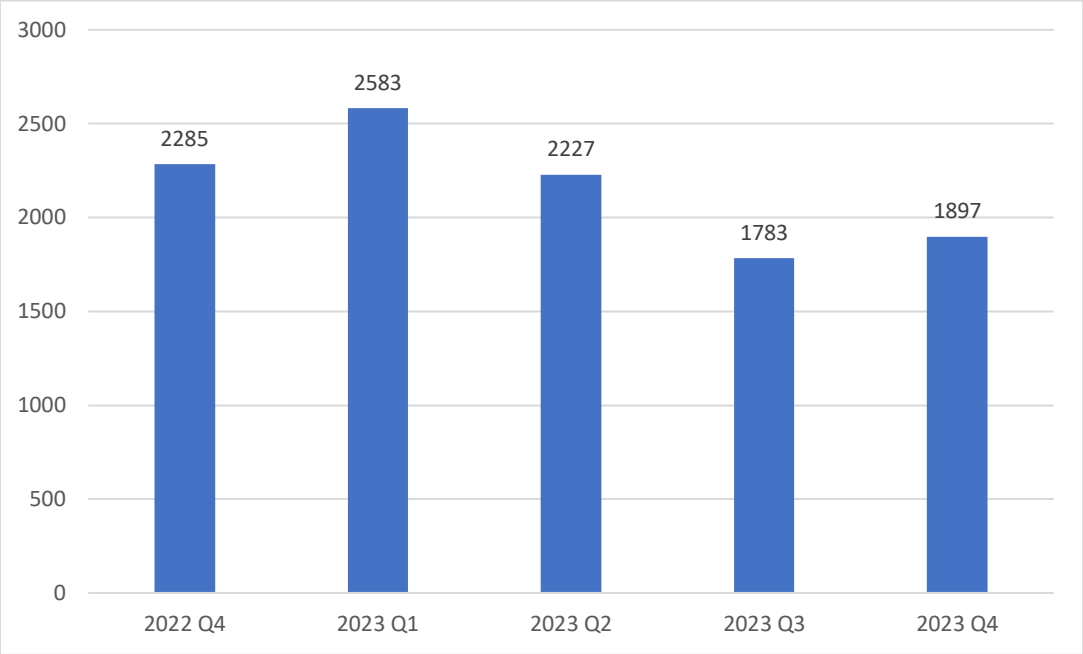
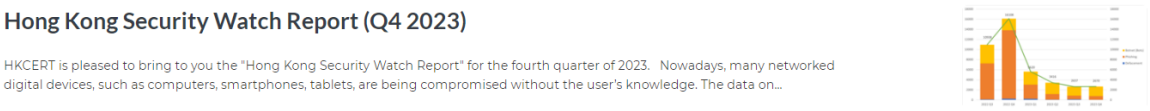


Figure 4. Trend of Bot related security events in the past year
(Source: data feeds from overseas security researchers, not from incident reports)

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).

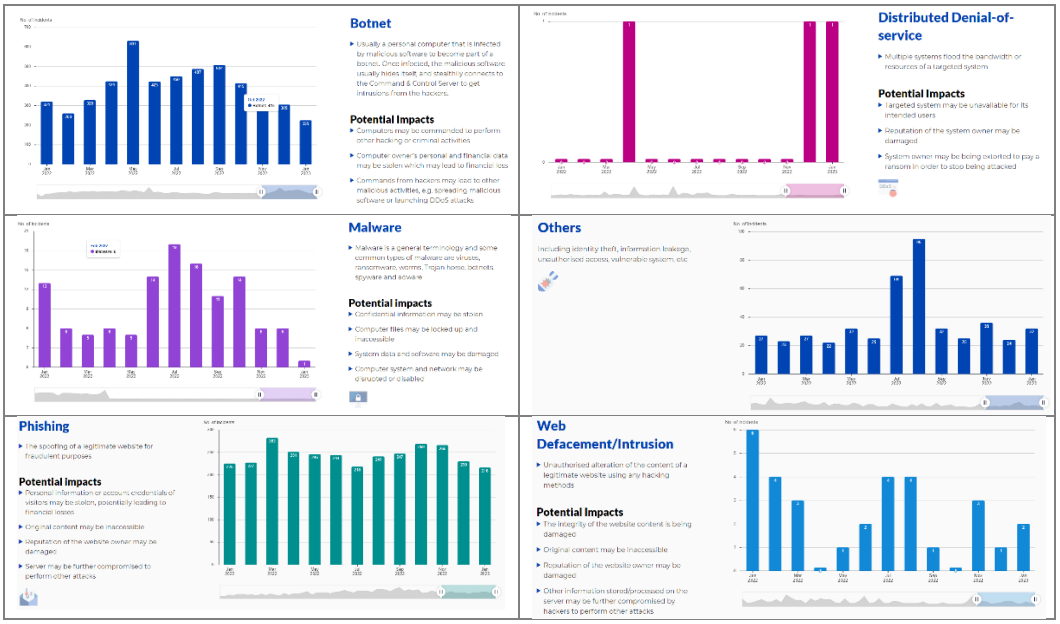


Figure 5. Charts in HKCERT website showing the statistics of different types of incident reports.

4. Events organised and co-organised

4.1 Build a Secure Cyberspace 2023

HKCERT jointly organised the “Build a Secure Cyberspace 2023” campaign with the Government and Hong Kong Police Force. The campaign involved 2 public seminars, and a speech contest. An award presentation ceremony was organised in Sep 2023.

For the Folder Design Contest, HKCERT received about more than 150 applications from Open Group, Secondary School and Primary School Group. A professional judge panel selected winners with most creative and meaningful. Figure 6 shows the photos of winners receiving the rewards.

Primary Group	Secondary Group
	

Open Group


Figure 6. Winners of Primary School, Secondary School, Open Categories received the rewards.

Use this link to access the winning entries online:
https://www.cybersecurity.hk/en/contest-2023.php

4.2 Capture The Flag Contest

HKCERT jointly organised the “Hong Kong Cyber Security New Generation Capture the Flag Challenge 2023” (HKCERT CTF 2023) with partner associations in information and education sectors. The 48-hours contest was opened to all participants who were enthusiastic with Capture the Flag. This year, HKCERT CTF 2023 was firstly opened to international to register. It was a success with more than 500 teams and close to 1,100 participants from universities, secondary schools and open categories, also from international. A public seninar with award ceremony was organised in December 2023. Furthermore, it received prestigious acclaim from SECCON CTF 2023, a flagship CTF competition in Japan. The winning team of HKCERT CTF 2023 received a special privilege of bypassing the qualifying round and participated directly in the international finals taking place in Tokyo during Christmas of 2023.

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-2023-seminar-and-award-presentation-ceremony

4.3 "All-Out Anti-Phishing" Moving Showroom Campaign

Moving showroom campaign involved 3 phases and over 10 different locations in Hong Kong. HKCERT crossed over DinDong designer to design an anti-phishing themed moving showroom. The campaign visited Hong Kong, Kowloon, and the New Territories to teach citizens how to identify and prevent phishing attacks. Thousands of residents visited the showroom with positive feedback.

4.4 Smart City Roving Exhibition

Smart city roving exhibition was organized by Hong Kong government. HKCERT was on of the participant. It involved how various smart city initiatives in Hong Kong can bring convenience to their daily life through the adoption of technology. In the exhibition, HKCERT held a booth to raise the awareness of cyber security among the public.

4.5 Innocarnival 2023

Innocarnival 2023 was organised by Innovation and Technology Commission. HKCERT held a booth in the activity and interacted with the public via deepfake technology.

5. Collaboration

5.1 International Collaboration

HKCERT participated in a number of international coordination and collaboration events in year 2023:

- Participated in the NatCSIRT Conference 2023
- Participated in the AusCERT Conference 2023
- Participated in the HITCON 2023

- Participated in the 2023 APCERT Cyber Security Drill Exercise
- Participated in the APISC Security Training Course 2023
- Participated in the APCERT AGM and Conference 2023
  - Presented “Raising Cyber Security Awareness – A Localised Approach”
- CNCERT Annual Conference
  - Presented “Hong Kong SME Cyber Security Connection Programme ”
- Participated in the SECCON 2023
- Participated in the JSAC 2024

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 October 2023. 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 Comprehensive Guide to Social Media Scams

HKCERT had launched the "Comprehensive Guide to Social Media Scams: Setting up Defense to Safeguard Your Personal Information" (https://www.hkcert.org/security-guideline/comprehensive-guide-to-social-media-scams-setting-up-defense-to-safeguard-your-personal-information) in Aug 2023. The guideline covered information of 2 areas to aid user to handle social media scams. These 2 areas include (1) Phenomenon of social media scams, and (2) Preventative measures to social media scams, also how to report the scams on social media platforms.

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 Ransomware Trend

HKCERT studied and analysed the ransomware trend across asia-pacific . Advisories were published to raise situational awareness of users for the prevention and detection measures. (https://www.hkcert.org/blog/ransomware-trends-q2-2023-surge-in-attacks-across-asia-pacific-persistent-multiple-extortion-and-evolving-threat-landscape)

6.6 Security Guidelines and Advisories for Security Outlook 2023

HKCERT published different security guidelines and alerts in response to the cyber threats and incidents mentioned in “Year Ender Press Briefing 2023”, such as identity or credential theft , attacks using artificial intelligence, crime-as-a-service, attacks targeting Web 3.0 and attacks targeting IoT.

6.7 HKCERT “All-Out Anti-Phishing” Thematic Page

HKCERT would like to reinforce our target of preventing phishing through educating the public. Therefore, HKCERT introduced a new thematic page "All-Out Anti-Phishing" (https://www.hkcert.org/publications/all-out-anti-phishing). The thematic page consolidates all essential information about phishing, including attack techniques, prevention, identification, and handling procedures for suspicious messages.

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 devices.

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 2024 to review cyber security landscape of 2023 and provided an outlook to 2024 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 2024/2025. We shall work closely with the Government to plan for the future services of HKCERT and seek their support.

7.3 Enhancement Areas

HKCERT will launch "Cyber security on the Trams". HKCERT will invite participants from open group, secondary school and primary school groups to design the outlook of the tram, following the theme of cyber security. The designs of the winners will be displayed on the physical trams.

HKCERT will launch a cyber security public awareness campaign called "Cyber Security Week". A big exhibition will be held in a shopping mall with different display booths and interactive games.

HKCERT will hold a large cyber security drill exercise with critical infrastructure shareholders.

HKCERT will continue to work on IoT research. Electronic billboards will be our target.

HKCERT will continue to organise the Capture the Flag (CTF) contest, HKCERT will continue to partner with different associations to organise another CTF in 2024 for the participants from universities, secondary schools and open categories.

8. Conclusion

In 2023, the number of overall security incidents reported to HKCERT dropped by 8% and went back to level of 2021. The phishing cases and phishing URLs recorded a rise, increased by 27% and 22% respectively. It became the first major security incident in Hong Kong. It was believed that the rise came from phishing campaigns targeting reward programs owned by Hong Kong organistaions. Botnet just recorded a decrease. The reason was complicated and under investigation.

In 2024, 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 2024:

1. **"Weaponisation" of AI**: Hackers use generative AI to issue instructions for generating malicious code, dominating cyber attacks. Additionally, hackers can use AI to generate disinformation that affects the output of other AI, bypassing cyber security measures. Hackers also use AI to create fake videos to deceive for personal gain.

2. **Next-Level Phishing Attacks**: In addition to using traditional methods such as emails and text messages to conduct phishing attacks, hackers also use fake videos to impersonate someone's identity. Phishing attacks also extend to social media platforms, impersonating some brand pages. At the same time, hackers use search engine optimisation (SEO) techniques to make phishing websites appear at the top of search results, deceiving more victims.

3. **Trend towards Organised Cybercrime**: In 2023, Hong Kong experienced several ransomware attacks targeting local organisations, resulting in large

amounts of ransom being extorted and sensitive data being exposed. Citizens also faced threats from malicious apps and phishing. Globally, the number of ransomware attacks and vulnerabilities reached a new high in 2023, indicating an increasingly serious trend of organised and systematic cybercrimes.

4. **Attacks Arisen from Smart Devices**: Electronic products nowadays are most equipped with network connectivity, allowing them to connect to other devices or the internet. These products have varying cyber security standards and are susceptible to intrusion and malicious manipulation. Some products cannot patch security vulnerabilities, making them difficult to block cyber attacks.

5. **Third-party Risk**: Most companies use IT services provided by third-party, such as software and IT personnel, but this gives rise to IT supply chain attacks and insider threats, leading to data breaches, ransomware attacks, and other consequences. Additionally, research suggests that generative AI may produce incorrect information, such as code with security vulnerabilities or false information. If organisations adopt such information without verification, it brings risks to their operations.

-- END --