ANNUAL REPORT 2025

香港網絡安全事故協調中心

Hong Kong Computer Emergency

Response Team Coordination Centre

Hong Kong Productivity Council

HKCERT Annual Report 2025

1. Highlights of 2025

1.1 Summary of Major Activities

- Organised the “Build a Secure Cyberspace 2025 - Let’s Secure as we Digitalise” campaign with the Digital Policy Office and Hong Kong Police Force.
- Launched Cybersecurity Service Providers Connect Programme
- Organised the “HKCERT Capture the Flag 2025”
- Presented in different international conferences and local press briefing.
    - “Year Ender” in local media briefing to call on public to raise awareness of cybersecurity
    - 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 emerging technology

1.2 Achievements & Milestones

- Organised the “Build a Secure Cyberspace 2025 - Let’s Secure as we Digitalise” campaign with the Digital Policy Office and Hong Kong Police Force. The campaign featured one webinar, one public seminar, an instant messaging Apps stickers design contest, and an award presentation ceremony. The contest attracted over 2,000 participants while more than 600 participants attended the webinar and seminar.
- Launched Cybersecurity Service Providers Connect Programme. The programme is a long-term initiative designed to connect service providers with enterprises and build a trusted ecosystem. To date, more than 20 service providers have met the requirements and are now listed on the platform.
- Organised “HKCERT Capture the Flag 2025”. The HKCERT Capture the Flag 2025 event featured 3 workshops, a 48-hour online qualifying contest, a 1 day in-person competition for the finals with an award ceremony. This year was the first time the competition incorporated both attack and defence elements, making the format much closer to real-world scenarios. The event drew a record-breaking

1,900 participants from worldwide.

- Published security advisories on latest risks on emerging technology and emerging cyber threats
- Continued the Healthcare Cyber Security Programme and Critical Infrastructure Cyber Security Programme.

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), 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 2025, HKCERT had handled 15,877 security incidents which was 27% increased of the previous year (see Figure 1).

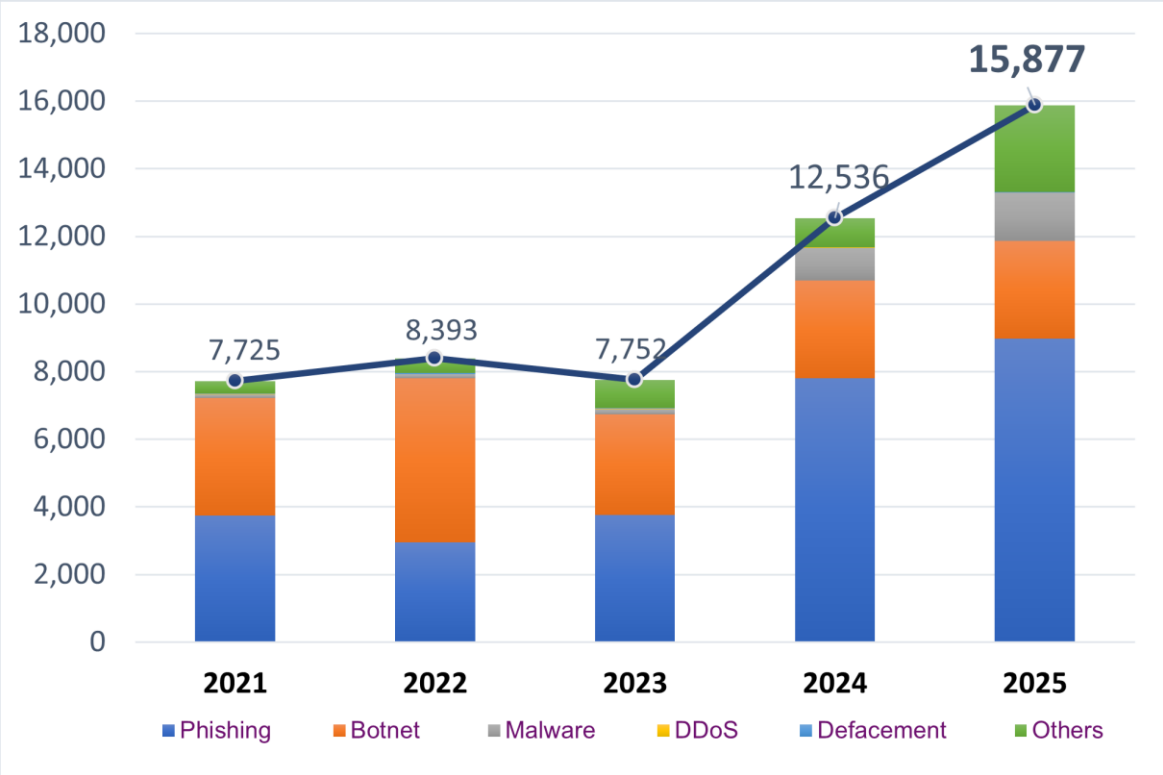

Figure 1. HKCERT Security Incident Reports

While the number of overall security incidents handled by HKCERT broke the record in 2025. It was the first time to hit over 15,000 cases. Phishing (8,973 cases or 57% of total cases) went up 15% and total phishing URLs was increased by 29%. Phishing primarily targeted the social media, instant messaging sectors, followed by crypto, banking, tech enterprises and e-commerce respectively. Malware incidents also rose significantly in 2025, increasing 3.6-fold year-over-year, with most cases involving trojans targeting smart devices disguised as legitimate applications.

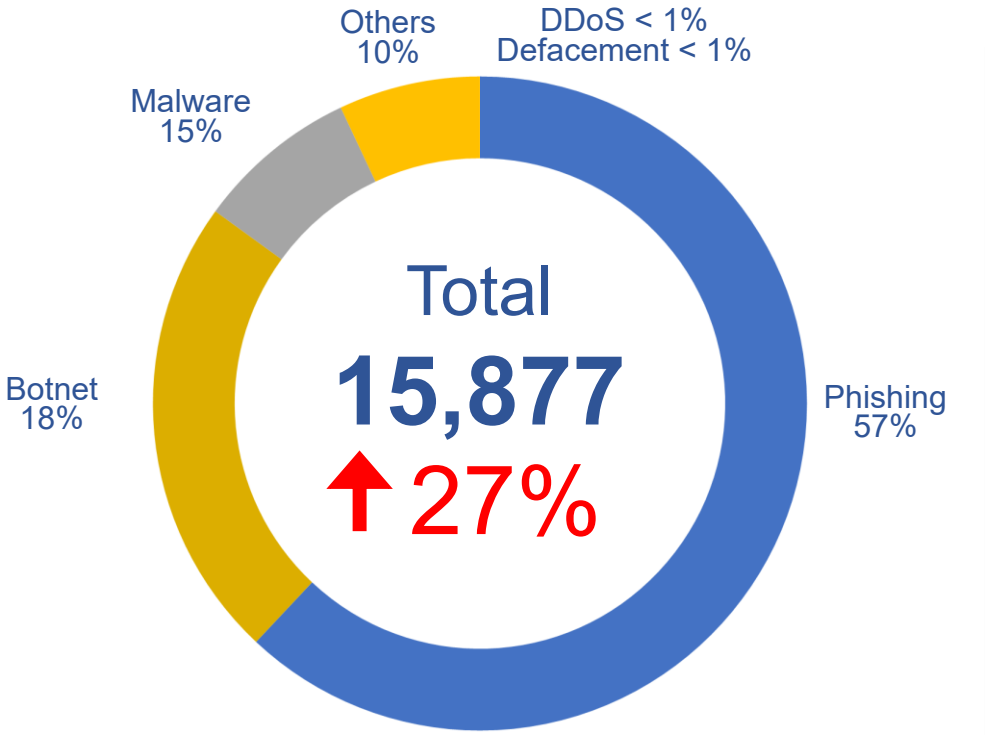

Figure 2. Distribution of Incident Reports

3.2 Watch and Warning

During the period from January to December of 2025, HKCERT published 415 security bulletins for the vulnerabilities of major software (see Figure 3) on the website. In addition, HKCERT have also published 22 security advisories, topics such as risks from third-party and weaponisation of AI.

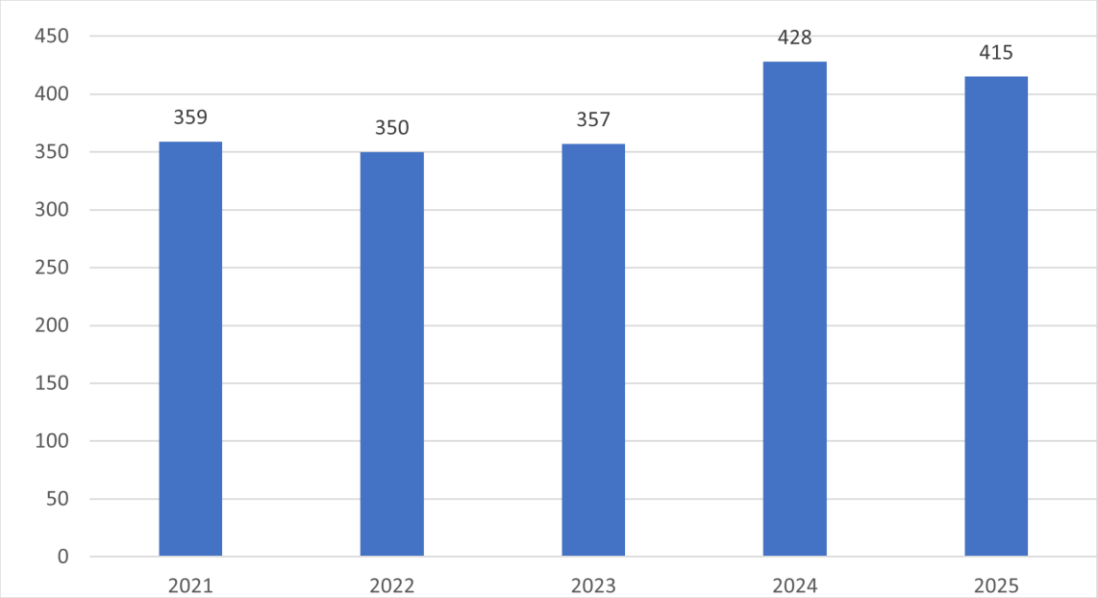

Figure 3. HKCERT Published Security Bulletins

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 detected in IFAS.

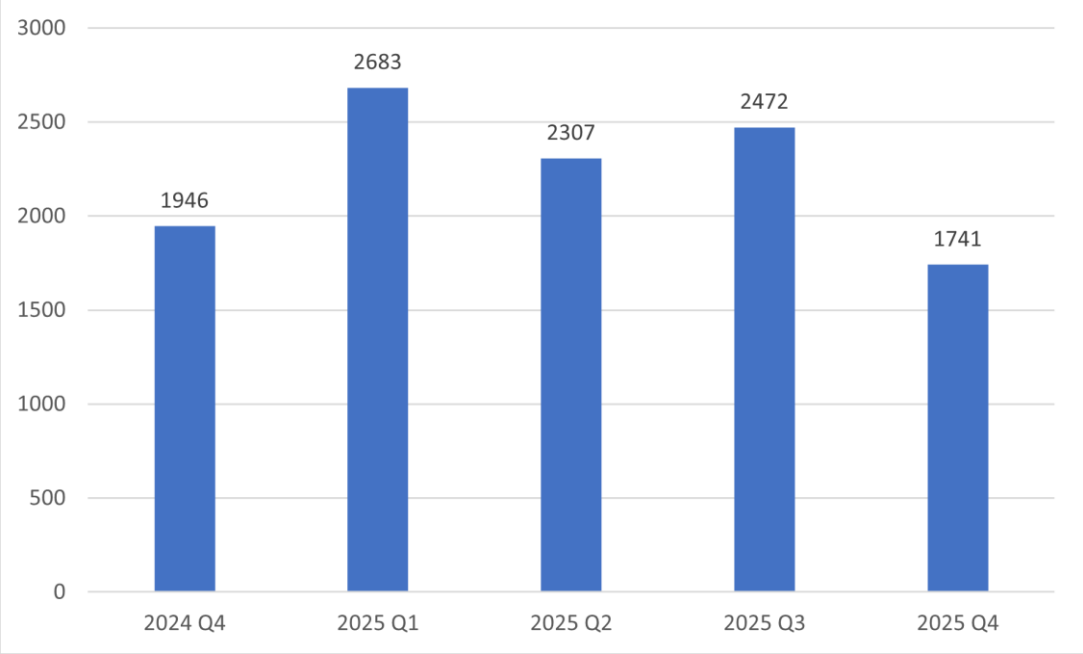

Figure 4. Trend of Bot related security events in the past year
(Source: data feeds from overseas security researchers, not from incident reports)

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 month (see https://www.hkcert.org/statistics).

4. Events organised and co-organised

4.1 Build a Secure Cyberspace 2025 – Let's Secure as we Digitalise

HKCERT jointly organised the “Build a Secure Cyberspace 2025” campaign with the Digital Policy Office and Hong Kong Police Force. The campaign involved 1 webinar, 1 public seminar and an instant messaging Apps stickers design contest. An award presentation ceremony was organised in Sep 2025.

For the instant messaging Apps stickers design contest, HKCERT received about more than 2,000 applications from Open Group, Secondary School and Primary School Group. A professional judge panel selected winners with most creative and meaningful.

Winning entries: https://www.cybersecurity.hk/en/contest-2025.php)

4.2 Cybersecurity Service Providers Connect Programme

The "Cybersecurity Service Providers Connect Programme (CSPCP)," launched by the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), is designed to link local cybersecurity service providers with enterprises and institutions via a dedicated platform. This initiative streamlines the search for cybersecurity solutions and promotes the growth of the local cybersecurity ecosystem.

On 23 October 2025, the programme was officially launched, and more than 20 service providers participated the programme until now. On 22 January 2026, CSPCP organised a seminar featuring exhibition booths and panel discussions, attracting over 100 participants who visited the service provider booths. HKCERT will continue to engage more service providers to build up a trusted ecosystem.

(Programme Website: https://spconnect.hkcert.org/)

4.3 HKCERT Capture the Flag 2025

The “HKCERT Capture the Flag 2025” partnered associations in information and education sectors. It was opened to all participants who were enthusiastic with Capture the Flag. This year, it was the first time for HKCERT CTF to introduce attack and defence elements. It was a success with more than 600 teams and 1,900 participants from universities, secondary schools, open categories and international. Following the final round, a public seminar with award ceremony was held in February 2026.

(Winners: https://www.hkcert.org/event/hkcert-capture-the-flag-challenge-2025)


HKCERT Capture the Flag Challenge
香港網安奪旗賽
RT Capture The Flag Challenge
香港網安奪旗賽

5. Collaboration

5.1 International Collaboration

HKCERT participated in a number of international coordination and collaboration events in year 2025:

- Collaboration Meeting with CNCERT
- Participated in the AusCERT Conference 2025
- Participated in the FIRST Conference 2025
- Participated in the NatCSIRT Conference 2025
- Participated in 2025 APCERT Cyber Security Drill Exercise
- Participated in HITCON 2025
- Participated in CNCERT Annual Conference
- Participated in APCERT AGM and Conference
- Collaboration Meeting with MNCERT/CC

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 2,000 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 two Advisory Group Meetings in October 2025. The meetings 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 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.

6.4 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.

6.5 Year Ender Press Briefing

HKCERT organised a year ender press briefing to media in January 2026 to review cybersecurity landscape of 2025 and provided a cybersecurity forecast to 2026 to warn the public for better awareness and preparedness. It received very good press coverage.

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 2026/2027. 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 enhance the "Cybersecurity Service Providers Connect Programme" by introducing additional features, enabling organisations to more easily identify reputable service providers.

HKCERT will continue to strengthen public cybersecurity awareness, with new promotional campaigns planned for the coming year.

In addition, HKCERT will continue organising Capture the Flag (CTF) competitions. In 2026, HKCERT will partner with various associations to host another CTF for university students, secondary school students, and open-category participants.

8. Conclusion

In 2025, the number of overall security incidents reported to HKCERT increased by 27% and broke the record. The phishing cases and phishing URLs recorded a rise, increased by 15% and 29% respectively. It became the first major security incident in Hong Kong. Malware cases also recorded a rise, increased by 3.6-fold due to adding new sources of threat intelligence.

In 2026, 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 such as Capture the Flag competition, 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 2026:

1. **AI-Driven Attacks and Agentic AI Risks:** With rapid advancements in AI technology, cyber attackers are increasingly leveraging AI to launch more sophisticated attacks. Particularly agentic AI systems—which possess autonomous learning and execution capabilities—can make judgments and act on their own without human intervention. Once hacked, they will carry out potentially malicious commands automatically. These traits make such attacks harder to predict and defend against.

2. **Weak AI Governance of Enterprises Increases Data Leakage Risks:** Some enterprises lack clear internal guidelines regarding the use of AI. As a result, sensitive information—such as customer data and contract details—may be leaked if employees misuse public AI platforms. In certain cases, employees have used unauthorised AI tools or lacked understanding of the AI platform's privacy statement, thereby misjudging data security, entering sensitive data and unintentionally causing information leaks.

3. **Supply Chain Vulnerabilities and Third-Party Security Gaps:** Companies are increasingly relying on outsourced services and third-party platforms to

handle their business processes during operations. However, when these partners fall victim to cyberattacks or suffer from security flaws, the impact can cascade against client organisations. Even companies with strong internal cybersecurity measures may be compromised indirectly due to weaknesses in their supply chain.

4. **Over-Reliance on Cloud Infrastructure Creates Single Points of Failure:** Cloud platforms have become essential to enterprise operations, supporting data storage, application deployment, communications, and backups. However, over-dependence on a single cloud provider without adequate redundancy or contingency planning can be dangerous. In the event of a platform outage or service disruption, businesses may face complete operational paralysis.

5. **Emerging Threats from AI-Enabled Devices**: As AI-enabled devices (e.g., voice assistants, office robots, and customer service bots) are more integrated into business operations, they are revealing new security vulnerabilities. These devices usually employ Large Language Models (LLMs) to understand and parse human commands. With LLMs being embedded in physical systems, security vulnerabilities that originally existed in the digital environment may extend into the real world. Without strict authentication mechanisms in place, they are susceptible to voice spoofing or erroneous instructions, potentially triggering harmful actions.

-- END --