GovCERT.HK

Annual Report 2015

Contact:
cert@govcert.gov.hk

GovCERT.HK (www.govcert.gov.hk)

Government Computer Emergency Response Team Hong Kong – Hong Kong, China

1. Highlights of 2015

1.1 Summary of Major Activities

On 1 April 2015, the Government Computer Emergency Response Team Hong Kong, GovCERT.HK, was formed and officially commenced its services to centrally coordinate incident responses for over 80 departmental Information Security Incident Response Teams (ISIRTs) of the Government of the Hong Kong Special Administrative Region (HKSAR Government) as well as to step up collaboration with local and global Computer Emergency Response Teams (CERTs) to bolster cyber security capabilities of the territory.

1.2 Achievements and Milestones

As a new governmental CERT organisation, the GovCERT.HK proactively attended the NatCSIRT 2015, FIRST Annual Conference 2015, and APCERT AGM & Conference 2015, and subsequently succeeded in registering as a national CERT of CERT/CC, and joining as a full or operational member of FIRST and APCERT respectively.

Since its establishment, the GovCERT.HK has built up close working relationship with the CERT community and has been working smoothly on handling alleged security threats and imminent cyber attacks.

2. About GovCERT.HK

2.1 Introduction

The Government Computer Emergency Response Team Hong Kong, GovCERT.HK, is a governmental CERT responsible for coordinating incident response for the HKSAR Government.

Locally, the GovCERT.HK works closely with the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) on sharing of threat information and organising public awareness activities. The GovCERT.HK focuses on government-related matters while the HKCERT provides incident response related services to all

ICT users in the HKSAR covering public and private sectors as well as individuals.

Globally, the GovCERT.HK collaborates with the CERT community in sharing of incident information and threat intelligence; participating in training events, workshops and forums; and organising public awareness promotion activities and capability development initiatives.

2.2 Establishment

The GovCERT.HK was formed in April 2015 through consolidation of different internal IT security teams within the Office of the Government Chief Information Officer (OGCIO) of the HKSAR Government.

2.3 Resources

The GovCERT.HK is an establishment under the OGCIO and funded by the HKSAR Government.

2.4 Mission and Constituency

Being the governmental CERT, the GovCERT.HK will centrally manage incident response within the HKSAR Government and develop CERT-related services to enable government departments to understand the associated risks of information and cyber security, acquire necessary skills and take appropriate actions to protect government's information infrastructure and data assets.

3. Activities and Operations

3.1 Scope of Services

The GovCERT.HK is the computer emergency response team for the HKSAR Government, providing centrally managed incident response services; providing timely security advice; coordinating cyber security drills; promoting public awareness and capability; and engaging global CERT community with a view to enhance information and cyber security in the region.

3.2 Incident Handling Reports

In 2015, the GovCERT.HK have received and handled various types of information security incidents that are related to HKSAR Government installations. The issues varied from vulnerable websites, malware infection, web defacement, distributed denial-of-service (DDoS) attack, fraudulent emails, unauthorized access and loss of computing devices.

3.3 Alerts and Advisories

Since the establishment of the GovCERT.HK in April 2015, the GovCERT.HK issued 62 product security alerts, eight security reminders, and one security advisory requesting the disablement of SSLv3 protocol.

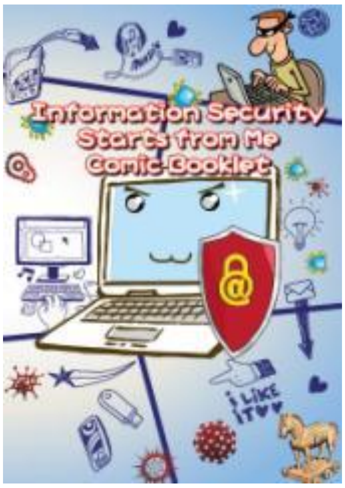
3.4 Publications and Mass Media

To raise public awareness and knowledge on the importance of information security, we resorted to different promotion channels to reach out to our target audience and collaborated with the industry players during the process.

- In order to raise the awareness of youth, information security promotional materials such as leaflets, booklets, and posters were distributed to all primary and secondary schools in Hong Kong and Scout Association of Hong Kong.
- Radio episodes entitled "e-World Smart Tips" were broadcasted to help the public to understand more about information security in various aspects and raise the public awareness on information security. On each month, the

radio episode featured a different theme and associated tips subject to the recent security incidents or foreseeable cyber threats. For instance, the tips of "Beware of Online Traps for Holidays" were broadcasted in December 2015 to remind the public about cyber traps before the Christmas.

- "Information Security Starts from Me" Comic Booklet with practical cyber security tips was published at the Cyber Security Information Portal to encourage readers to understand more on information security risks and the preventive measures while enjoying the comics. (www.cybersecurity.hk/en/resources.php)



- Leaflets were also produced with different promotion themes.

Smart You Smart Device
Awesome! Get pay apps for free!
Pay Game
Kekeke... Your device has been kidnapped. Ransom, please.
DATA LOSS or RANSOM
Apps from unknown source are dangerous. U know?
Of course.
So, I used the "DEMO" device to try. Easy to guess the device password "1234".
DEMO? That's mine.
RANSOM
Did you backup data?
Yes...but it's almost 2 years ago.
Secure Your Mobile Device
Cyber Security Information Portal
www.cybersecurity.hk

Please ☑ follow the security good practices below -

- ■ use strong password
- ■ enable security apps to detect malware
- ■ use up-to-date operating system, apps and web browsers
- ■ enable device encryption
- ■ remove unnecessary connection settings
- ■ restrict installation of mobile apps from unofficial sources
- ■ examine the permission requests of apps before installation
- ■ backup data regularly
- ■ stop location service if not necessary

Stay Alert!
Use Wi-Fi Network with Care
Wi Fi
Online Payment
Smart TV
Data Storage
Cyber Security Information Portal
www.cybersecurity.hk

Secure Your Wi-Fi Network

Please ☑ follow the security good practices below –

- □ update firmware and software of your devices, such as Wi-Fi routers and TV boxes regularly
- □ avoid using default settings in Wi-Fi routers, such as the default Service Set Identifier (SSID) and administrator password
- □ enable strong security for Wi-Fi communication, such as using WPA2 with AES 256-bit encryption
- □ enable built-in firewall of Wi-Fi router to protect your internal network
- □ turn off your Wi-Fi router if not in use

More advice for schools and small and medium enterprises (SMEs) –

- □ formulate policies on the proper use of Wi-Fi network and IT security instructions for end users
- □ enable MAC address filtering or other secure mechanisms for user authentication
- □ position Wi-Fi routers and wireless access points properly
- □ restrict access from guest Wi-Fi network to your internal network
- □ review log records regularly to detect suspicious events

- Social media, including Twitter and Facebook, were used to share news on information security and promote upcoming security seminars and events.
- Security alerts and advisories were published on the GovCERT.HK website (www.govcert.hk) to provide latest information on security threats and vulnerabilities for the public to take appropriate actions in response.

4. Events Organized / Hosted

With the objectives to continuously enhance information and cyber security capabilities of the HKSAR Government, the GovCERT.HK regularly organises awareness training and solution workshops to share latest knowledge on security measures, best practices, skills and security solutions with government users.

4.1 Training

Over 12 security awareness seminars and training were organised in 2015 to ensure that government staff remains vigilant in protecting their systems and safeguarding sensitive information.

- Seminars and showcases were conducted for government IT staff and users to raise their security awareness and introduce the latest IT security technologies and solutions. The topics included industry best practices, mobile and cyber security, data protection, end-point protection and anti-DDoS solutions
- Seminars were organised for departmental IT security officers to refresh their security knowledge and update them on the Government's latest approaches in dealing with cyber security threats and adopting mitigation measures.
- Professional web application security training and sharing sessions for government IT staff were arranged. The sessions specifically addressed common weaknesses of websites and web applications, and offered practical advice on the corresponding improvement measures to upkeep information security at a high level.

4.2 Drills and Exercises

The GovCERT.HK actively coordinated government departments to conduct cyber security drills to assess the participants' capabilities of incident analysis, the standing incident response procedures with a view to enhancing the overall incident response capabilities. In 2015, we conducted eight drill exercises involving different government departments and their respective services contractors.

4.3 Conferences and Seminars

In 2015, the GovCERT.HK adopted the slogan "Cyber Security is Everywhere" as the key message to government users and the public. The target audience included businesses especially small and medium enterprises (SMEs), organisations, schools, and general public.

- Two seminars were organised under the "Build a Secure Cyberspace" campaign in April and November 2015, aiming to promote public awareness of information security and the adoption of security best practices. The one-day seminar in November 2015 has 13 sessions covering trends in cyber crimes, information security challenges, threats related to mobile banking, mobile and smart device security, cloud security, and security measures to combat cyber attacks.
- A security seminar with the theme of "Cyber Crime Prevention, Information Security Best Practice for SME and e-Commerce" was conducted to raise the awareness of SMEs in cyber crimes and share information security best practices in September 2015.
- 25 seminars were conducted at primary and secondary schools from June 2015 to December 2015 for 10,870 teachers, parents and students to raise their awareness of cyber security and enhance their knowledge of protecting personal information.
- A graphic design contest with the theme "Cyber Security is Everywhere" was organised from June 2015 to October 2015 to promote public awareness of information security and security best practices, and appeal to the public to be vigilant and thereby avoid falling into the trap of criminals. The winning entries of the contest were posted at the Cyber Security Information Portal to continue the promotion effect (www.cybersecurity.hk/en/contest-2015.php).
- A talk was delivered at a seminar of Mass Transit Railway Corporation in July 2015 to raise their awareness of phishing and ransomware and provide advice on protection against those attacks.

5. Local and International Collaboration

The GovCERT.HK has been working closely with the HKCERT and other regional and global CERTs for coordinating threat information sharing and incident response.

5.1 Local collaboration

To raise public awareness, the GovCERT.HK collaborated with the HKCERT and security service providers to gather information on security vulnerabilities and timely issue alerts on malicious cyber activities to the public and private sectors.

The GovCERT.HK also steered the Internet Infrastructure Liaison Group (IILG) with members from Internet infrastructures (including Hong Kong Internet Exchange, and the Hong Kong Internet Registration Corporation Limited), major Internet service providers, and stakeholders to closely monitor the Internet operation status with a view to mutually alert on abnormal activities.

5.2 International Collaboration

To foster the Government’s collaboration with international security experts for sharing experience in information security and strengthening knowledge of emerging cyber threats, vulnerabilities and appropriate mitigation solutions, the GovCERT.HK strives to learn from the CERT community on global development in international standards development, global information security and data privacy policies, cyber crime initiatives, and technological researches.

The GovCERT participated in the following activities in 2015:

- Attended NatCSIRT Annual Technical Meeting and registered as a national CSIRT in June 2015.
- Attended FIRST Annual Conference 2015 in June 2015 and registered as a full member in October 2015.
- Attended APCERT Annual General Meeting and Conference in conjunction with Organisation of Islamic Cooperation (OIC-CERT) and registered as an Operational Member in September 2015.
- Attended the APCERT on-line training on “Debugging and Exploiting

Security Vulnerabilities on Routers" in October 2015 and on-line training on APCERT drill in December 2015.

- Attended and delivered a speech at the Cloud Security Alliance Asia Pacific (CSA APAC) Congress in December 2015.
- Subscribed to the mailing lists of APCERT and FIRST.
- Participated in the Information Sharing Working Group of APCERT.

6. Future Plans

6.1 Future Projects

The GovCERT.HK will explore appropriate tools and solutions to establish a cyber health index as a base reference on the cyber security landscape of Hong Kong. We will also explore the need to implement an information sharing and analysis platform with big data analytics capability to cope with the massive information flow of security intelligence with a view to formulating early warning for our stakeholders in an efficient and effective manner.

Apart from general public awareness training and promotion initiatives, the GovCERT.HK will work with local universities and the industry to organise a cyber security competition entitled "Build a Secure Cyberspace 2016" to promote awareness of information security and proper cyber etiquette.

6.2 Future Operation

The GovCERT.HK will continue to expand its operations appropriately to cope with anticipated workload generated from the increasing security threats and alleged cyber attacks in the region.

7. Conclusion

In light of the proliferation of hacking activities and growing complexity in each incident, it is essential for the GovCERT.HK to establish and maintain close collaboration and operations with local and global CERTs to meet the ever-increasing challenges on cyber security. The GovCERT.HK will strive to work closely with the industry, professional organisations, and various stakeholders to maintain a secure, stable and trustworthy cyber world for people from all walks of life.