

GovCERT.HK

Annual Report 2017



1. Highlights of 2017

1.1 Summary of Major Activities

In 2017, we completed the review of the standing Practice Guide for Information Security Incident Handling with reference to the ISO 27000 standards and promulgated for reference by all our constituents. We also co-organised with the Hong Kong Police Force (HKPF) to run an inter-departmental cyber security drill and walk through the procedures of security events analysis and incident response with our constituents to enhance the overall capability of the Government of the Hong Kong Special Administrative Region (HKSAR Government) in incident management.

In response to the soaring increase of ransomware outbreak during the first half of 2017, we developed dedicated best practices, thematic leaflets, and defensive guidelines for all government users as well as lined up security solutions providers to share with our constituents the latest cyber resilience technologies and best practices to protect information systems from zero day exploit. We also joined with the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) to promote awareness of ransomware and malware attacks through a dedicated “Fight Ransomware Campaign”. The “Ransomware Intelligence Portal” was built on social media to share latest risk information and actionable advice with the general public.

To strengthen our capacity in cyber threat monitoring and assessment, we established a cyber risk information sharing platform to centrally manage cyber threat intelligence and actionable advice for the consumption by our constituents. We have reviewed and enforced a cyber threat assessment framework for reference by both internal and outsourced security practitioners so that aligned actions would be derived when pre-defined conditions were met. We also published security alerts and mitigation advice through the Government Computer Emergency Response Team Hong Kong (GovCERT.HK) web portal for reference by the general public.

In February 2017, we hosted a Collaboration Meeting with Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) and HKCERT and invited JPCERT/CC to run a TSUBAME technical workshop to explore collaboration in threat hunting.

1.2 Achievements and Milestones

Cyber Threat Assessment and Incident Management

GovCERT.HK started to publish Weekly IT Security News Bulletins since January 2017 to highlight security information including vulnerabilities, security patches, malicious activities and security incidents that might have impact to government information systems and Internet-based services.

When needed, GovCERT.HK would issue security alerts as early warnings and request government IT users to take appropriate actions accordingly. For easy interpretation on our security alerts, we have reviewed and published the “Cyber Threat Assessment Framework” as a reference tool used to describe, analyse, assess, rate and prioritise various risks by estimating the probability of occurrence and the severity of impact if they occur. The Framework is as follows.

		Threats		
		Low	Medium	High
		<input checked="" type="checkbox"/> Vulnerability reports received from sources <input checked="" type="checkbox"/> Malicious activities in the cyberspace identified by SIEM <input checked="" type="checkbox"/> Malware, phishing, web attack (Injection, XSS, DoS/DDoS) requiring user interactions <input checked="" type="checkbox"/> Only locally exploitable & Privileged access account required	<input checked="" type="checkbox"/> Alerts of targeted attack against the Government received from sources <input checked="" type="checkbox"/> DDoS/application attack against individual government website/system/network reported <input checked="" type="checkbox"/> Remotely exploitable via network & No user interaction required to launch attack <input checked="" type="checkbox"/> Privilege access elevation enabled	<input checked="" type="checkbox"/> Global outbreak report received from sources <input checked="" type="checkbox"/> DDoS/application attacks against multiple government websites/systems/networks reported <input checked="" type="checkbox"/> Exploit code publicly available & Exploitation reported/observed <input checked="" type="checkbox"/> Advanced persistent threat with privilege access elevation
Impacts	High	Security Alert Line-to-Take	High Threat Security Alert Line-to-Take Call for Actions	High Threat Security Alert Line-to-Take Call for Returns
	Medium	Security Alert	Security Alert	High Threat Security Alert Call for Actions
	Low	Vulnerabilities & Security Updates	Security Alert	Security Alert
		<input checked="" type="checkbox"/> Result in loss of classified data <input checked="" type="checkbox"/> Affect public-facing website/e-service <input checked="" type="checkbox"/> Attack could spread through internal network <input checked="" type="checkbox"/> Widely reported by local mass media		
		<input checked="" type="checkbox"/> Result in loss of data <input checked="" type="checkbox"/> Affect internal website/e-service <input checked="" type="checkbox"/> Attack spreads through Internet <input checked="" type="checkbox"/> Reported internationally but no local media coverage		
		<input checked="" type="checkbox"/> No service interruption <input checked="" type="checkbox"/> No data loss <input checked="" type="checkbox"/> Affect individual user/ internal application system <input checked="" type="checkbox"/> No media coverage		

Liaison and Collaboration

We have been proactively participated in the APCERT’s activities and worked closely with the CERT community in handling threat information. We also collaborated closely with HKCERT, CNCERT/CC, MOCERT, and JPCERT/CC in different initiatives and projects.

Cyber Threat Intelligence Management

From time to time, we received various cyber threat intelligence from different sources and gathered threat information from the public domain. To facilitate efficient and effective correlation of threat information and potential impact to the government information systems, we launched the Cyber Risk Information Sharing Platform (CRisP) in April 2017 as an information hub for use by all our constituents.

Riding on the Platform, we were piloting different big data analytics tools to support data collection, correction, and discovery of uncommon usage patterns. We have been piloting the development of different dashboards to facilitate security analysis and formulation of early warnings. The Platform also facilitates closed group discussion and knowledge sharing.

Awareness Building and Public Education

In view of the rising trend of ransomware attacks in 2017, GovCERT.HK developed thematic leaflets to recommend relevant precautionary measures and security controls for our constituents. For the wider community, we also set up thematic web pages at the “Cyber Security Information Portal” (www.cybersecurity.hk, the CSIP portal) on ransomware and posted detailed steps to protect themselves from and defend against ransomware attacks.

GovCERT.HK also devoted much attention to public education and capacity building in different business sectors and age groups. In 2017, we organised 32 school visits to reach out to around 10 000 students, parents and teachers.

2. About GovCERT.HK

2.1 Introduction

GovCERT.HK is a governmental CERT responsible for coordinating incident response for over 80 departmental Information Security Incident Response Teams (ISIRTs) of the HKSAR Government.

Since its establishment, GovCERT.HK has profoundly shaped the management framework and coordination mechanism of incident handling; and empowered close collaboration with the industry, critical Internet infrastructures, and the Computer Emergency Response Team (CERT) community for timely exchange of cyber threat information and coordinated response. GovCERT.HK also works closely with HKCERT and local industry on cyber threat intelligence sharing, capability development, public education, and continuous promotion on cyber security and resilience through social and mass media.

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

2.2 Establishment

GovCERT.HK was established on 1 April 2015 through the consolidation of internal IT security teams within the Office of the Government Chief Information Officer (OGCIO) of the HKSAR Government.

2.3 Resources

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

2.4 Mission and Constituency

Being the governmental CERT, GovCERT.HK will centrally manage incident response within the HKSAR Government and develop CERT-related services to assist government departments in understanding the associated risks of information and cyber security, implementing appropriate security measures, monitoring on potential threats and responding to security events with a view to ensure would be well protected.

3. Activities and Operations

3.1 Scope of Services

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

3.2 Security News Bulletins

In 2017, GovCERT.HK published the following regular security bulletins to raise the awareness among government users and the general public.

- “Security Vulnerabilities and Patches” information would be consolidated on every working day and disseminated to registered subscribers through emails;
- “Security Industry News” would be gathered on every working day and top news with wide impact would be compiled and disseminated to registered subscribers through emails; and
- “Weekly IT Security News Bulletins” would be published on the working day that starts each week to highlight top 2 to 3 security news during the week and summarises vulnerabilities by products for easy reference by security practitioners. These Bulletins would be distributed to registered subscribers through emails and posted at the GovCERT.HK website as public information (www.govcert.gov.hk/en/reports.html#weekly-reports).

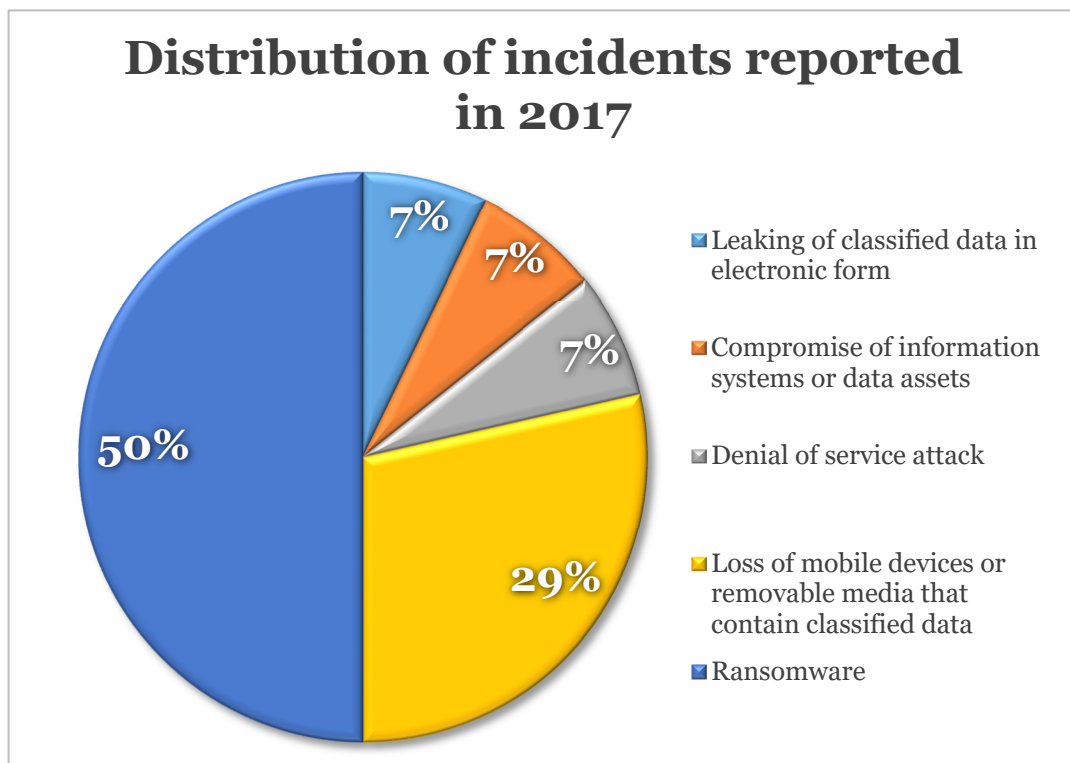
3.3 Alerts and Advisories

In 2017, we published 87 product security alerts associated with computing products widely deployed in government installations. We also released a security advisory for public reference highlighting the risk of the KRACK (Key Reinstallation AttaCKs) vulnerabilities and recommending appropriate measures to protect data confidentiality of Wi-Fi network connections (www.govcert.gov.hk/en/advisories.html).

In 2017, we conducted threat analysis on over 200 security events detected and received from various sources. The threat information was extracted and shared with relevant constituents for appropriate follow-ups.

3.4 Incident Handling Reports

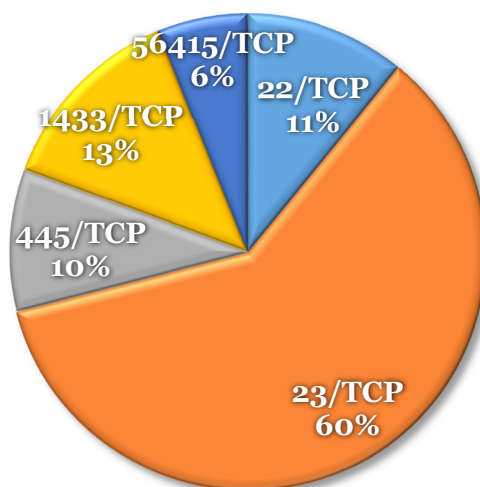
In 2017, GovCERT.HK received and handled various reports of cyber security incidents that were related to the government installations. The following chart shows the distribution of incidents reported in 2017.



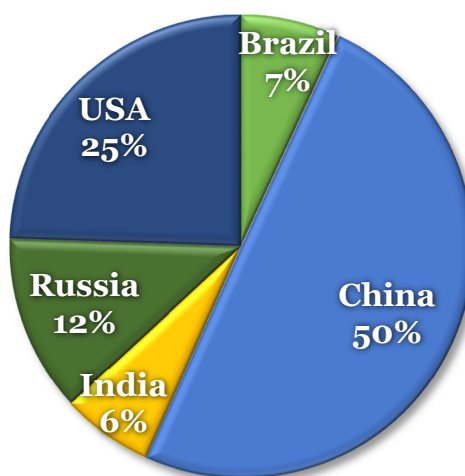
3.5 Abuse Statistics

As a member of the TSUBAME project, GovCERT.HK has set up sensors to collect and analyse network scanning activities targeting Hong Kong. The following charts show the top five scanning ports and the top five source regions of scanning activities detected by the TSUBAME sensors installed in Hong Kong.

Top 5 scanning ports against Hong Kong in 2017



Top 5 source regions of scanning against Hong Kong in 2017



3.6 Publications and Mass Media

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

- We broadcasted radio episodes entitled “e-World Smart Tips” to help the public understand more about information security in various aspects and raise their awareness of information security. The radio episode in each month featured a different theme and offered associated tips having regard to recent security incidents or foreseeable cyber threats. For instance, the radio tips of “Use mobile payment safely” were broadcast in September 2017 to remind the public on security measures in using mobile payment services.
- To provide practical tips and advice for Small and Medium Enterprise (SMEs) and the public to protect from cyber attacks, we developed and shared infographics covering popular security topics such as “Safe Online Shopping” to remind the public to take necessary precautionary actions to stay safe while shopping online.



(www.cybersecurity.hk/en/resources.php#infographics)

- A set of practical guidelines with different themes, including “HTTPS and Website Security”, and “Cloud Services Security and Privacy”, were produced to educate SMEs to deploying appropriate security measures in their business environment.



(www.cybersecurity.hk/en/resources.php#leaflets)

- We organised the “Smart Home, Safe Living” 1-Page Comic Drawing Contest with the theme “Smart Home, Safe Living” under the “Build a Secure Cyberspace” promotional campaign from April 2017 to September 2017. The contest has received overwhelming response with some 1 200 entries. A comic booklet and a 2018 calendar, adapted from the winning entries of the contest, were published to remind the public cyber security risks and suggest preventive measures through lively stories and figures.




www.cybersecurity.hk/en/resources.php#booklet

- To support and embrace the Domain Name System Security Extensions (DNSSEC) and Hyper Text Transfer Protocol Secure (HTTPS) technologies for better Internet security, adoptions of DNSSEC and HTTPS have been promoted to government websites to safeguard the online environment and strengthen trustworthiness of the websites. We have invited industry experts to contribute and share their insights on these topics and other hot issues at the “Expert Corner” of the CSIP. www.cybersecurity.hk/en/expert.php

EXPERT CORNER

Home > Expert Corner




Safeguarding your Domain Name with Domain Name System Security Extensions (DNSSEC)

According to statistics disclosed by the Hong Kong Computer Emergency Response Team Coordination Centre, the number of security incident reports increased by over 23% to 6,058 reported cases in 2016 compared with 2015...

Date : 26 September 2017
Organisation : Hong Kong Internet Registration Corporation Limited (HKIRC)
Writer : Mr Leo Lam, Chief Executive Officer of HKIRC

[More](#)



Moving More of the Web to HTTPS

HTTPS is an encrypted HTTP connection, making it more secure. If you own or run a website, implementing HTTPS is important to protect the integrity of your website and to preserve the privacy and security of your users...

Date : 3 Mar 2017 **Organisation** : Google Chrome **Writer** : Parisa Tabriz

[More](#)

4. Events Organised/Hosted

GovCERT.HK regularly organises awareness training and solution workshops to share latest knowledge on security measures, best practices, skills and security solutions with various levels of government users to continuously strengthen their knowledge on cyber attacks and enhance their information security skills, thereby strengthening their capabilities in guarding against cyber attacks.

4.1 Training

In 2017, we organised a total of 15 seminars, workshops and solution showcases for government IT staff and users to enhance their awareness of latest security vulnerabilities and update their knowledge in information security technologies.

- Seminars and showcases were conducted for government IT staff and users to raise their security awareness and introduce latest IT security technologies and solutions. The topics included industry best practices, ransomware and security of mobile applications.
- Seminars were organised for departmental IT security officers to refresh their security knowledge and update them on the Government's latest requirements and approaches in dealing with cyber security threats and adopting mitigation measures.
- Web vulnerability scanning workshops were organised for some 100 government officers to equip them with the necessary skills and knowledge to effectively identify the potential security weaknesses in web applications and remedy the security risks.

4.2 Drills and Exercises

GovCERT.HK has actively coordinated government departments to conduct cyber security drills to assess the participants' capabilities of incident analysis and test their incident response procedures with a view to enhancing the overall incident response capability.

In addition to conducting thirteen drill exercises involving individual government departments and their respective service contractors, we also conducted the inter-departmental cyber security drill in 2017 with some 40 departments participated to enhance the overall information security incident response capability of the Government. Using a number of simulated scenarios, the participating departments experienced how to respond to cyber security incidents effectively according to the established incident response procedure. In view of the success of this inter-departmental cyber security drill, the drill will be conducted regularly every year.

As the Operational Member of the Asia Pacific Computer Emergency Response Team (APCERT), GovCERT.HK participated in the APCERT Drill with the theme of “Emergence of a New Distributed Denial of Service Threat” in March 2017. GovCERT.HK played the role of Exercise Controller in addition to Player and Observer in the drill.

4.3 Conferences and Seminars

In 2017, GovCERT.HK adopted the slogan “Smart Home, Safe Living” as the key message to government users and the public. The target audience included businesses especially SMEs, organisations, schools and the public.



- Two seminars were organised under the “Build a Secure Cyberspace” promotional campaign in April and September 2017, aiming to promote public awareness of information security and the adoption of security best practices, in particular the risks of Internet-connected devices. The one-day seminar in September 2017 invited industry associations and experts to share insights on a range of security topics, including the most common cyber security threats nowadays, defence against ransomware, the secure use of mobile payment and social media.

- 32 school visits were conducted at primary and secondary schools in 2017, reaching out to some 10 000 students, parents and teachers for raising their awareness of cyber security and encouraging the proper attitude in using the Internet.



- To increase cyber security awareness among local primary, secondary and tertiary students on safe use of the Internet and social media, we supported the “Cyber Security Competition” in 2017 organised by the Hong Kong Police Force (HKPF) and the University of Hong Kong. The competition has received overwhelming response with over 7 600 participants. The competition included online quiz, security vulnerability analysis in simulated computers and presentation on topics related to cyber security.
- To promote the development of cyber security technologies and industry in Hong Kong and the Mainland, the second Hong Kong-Mainland Cyber Security Forum with the theme of “Facilitating Data Flow Securely and Orderly, Promoting Economic and Social Development” was held in October 2017. The forum attracted some 150 information security professionals from the Government, research institutions, the academia, professional organisations and the information security industry to exchange views on topics relating to data protection as well as personal data policy and law.

- To commend outstanding IT security professionals for their commitment and contribution in cyber security, we joined the HKPF and HKCERT to co-organise the second “Cyber Security Professionals Awards” (CSPA) in October 2017. Eighty cyber security managers and practitioners from five different sectors were elected to receiving the awards and merits. The following photo of the hosts and the judges was taken at the Awards Presentation Ceremony.
(www.csprofessionalsawards.net)



5. Local and International Collaboration

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

5.1 Local collaboration

To raise public awareness, GovCERT.HK collaborated closely with our partners such as HKPF and HKCERT, and security service providers to gather information on security vulnerabilities and promptly issue alerts on malicious cyber activities to the public and private sectors.

In view of the rising trend of ransomware attacks in recent years, GovCERT.HK and HKCERT jointly launched the “Fight Ransomware Campaign” in September 2017. The campaign featured the setting up of a “Ransomware Intelligence Portal” to share with the public the latest intelligence and analysis, security alerts and training information, etc. related to ransomware. As of December 2017, the campaign has conducted a total of four public seminars on ransomware and posted nearly 30 articles through the portal.

GovCERT.HK also plays a supportive role in the Internet Infrastructure Liaison Group (IILG) established and led by OGCIO. The key roles of the IILG are to maintain close liaison with Internet infrastructure stakeholders and strive in collaboration with the stakeholders for the healthy operation of the Internet infrastructure of Hong Kong. The IILG mechanism would be activated in support of major events or in response to incident outbreak or natural disasters that would affect the smooth operation of the Internet infrastructure of Hong Kong. In 2017, the IILG collaboration mechanism was activated six times in support of major events.

5.2 International Collaboration

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

In February 2017, GovCERT.HK hosted an International CERTs Collaboration Meeting with JPCERT/CC and HKCERT to share view on collaboration opportunity and invited JPCERT/CC to run a technical workshop on TSUBAME, the Internet threat monitoring system, with a view to support GovCERT.HK's cyber threat monitoring mechanism.



On 7 September 2017, GovCERT.HK signed an agreement with CNCERT/CC to receiving the China National Vulnerability Database information. This enabled GovCERT.HK to strengthen its capability in vulnerability analysis and management.

GovCERT.HK has participated in the following events in 2017:

- CNCERT/CC Annual Conference
- FIRST Annual Conference
- Annual Technical Meeting for CSIRTs with National Responsibility
- 2017 China Cybersecurity Week
- Hong Kong – Mainland Cyber Security Forum
- Microsoft Digital Crimes Consortium 2017
- Four APCERT on-line training sessions

6. Future Plans

6.1 Upcoming Projects

With the global upsurge in cyber security threats, GovCERT.HK will continue to stay vigilant in defending against potential cyber attacks. GovCERT.HK will explore appropriate tools and facilities to establish a testing centre for providing vulnerability scanning, penetration test, and malware analysis capability to protect government information systems.

6.2 Future Operations

GovCERT.HK will continue to forge closer ties and enhance information exchange with the CERT community, as well as streamline its operations to cope with the increasing security threats and alleged cyber attacks in the region. We will also explore the adoption of community-driven standards and protocols of Structured Threat Information Expression 2.0 (STIX2) and Trusted Automated Exchange of Intelligence Information (TAXII) to support effective threat analysis and exchange of cyber threat information in the long run.

To strengthen Hong Kong's overall capability in defending against and recover from cyber attacks, we will launch an initiative to promote territory-wide cyber security information sharing and collaboration. A pilot partnership programme for cyber security information sharing and collaboration will be launched to promote trusted partnership of local cyber security stakeholders across prominent sectors for sharing cyber threat information and security analysis on emerging cyber risks and vulnerabilities, as well as providing actionable insights to the community.

7. Conclusion

Cyber attacks become increasingly sophisticated and stealthy. GovCERT.HK has been proactively collaborating with local and global CERTs, making timely response and enhancing appropriate defensive measures to the imminent cyber security threats. GovCERT.HK would actively foster all stakeholders to take forward communication and exchange of cyber security information so as to keep abreast of the fast-evolving cyber security landscape and enhance the cyber security resilience capability of the community.

Contact: cert@govcert.gov.hk
Websites: www.govcert.gov.hk
www.cybersecurity.hk