APCERT Activities

Asia Pacific Computer Emergency Response Team

SC Leung
HKCERT
Chair organization / SC member of APCERT

AP* Retreat Hong Kong Meeting with Asia-Africa Forum (AAF)
20th February 2011

About APCERT

- **A**sia **P**acific **C**omputer **E**mergency **R**esponse **T**eam
  http://www.apcert.org
  - Forum of CERTs/CSIRTs in Asia Pacific region
  - Established in February 2003
  - Annual Events
    1. APCERT AGM & Conference
       - Exchange security trends & challenges
       - Local outreach and awareness raising for government & critical entities
    2. APCERT Drill (Simulation exercise of cyber attacks)
       - Communication check based on scenario
       - In conjunction with local exercise

  - APCERT Annual Report http://www.apcert.org/documents/index.html
    - Released every spring
    - APCERT teams' report on incident trends, statistics, new projects, and more

APCERT
Asia Pacific Computer Emergency Response Team

Objectives

- Encourage and support **regional and international cooperation** on information security in the Asia Pacific region;
- Jointly develop measures to deal with **large-scale or regional network security incidents;**
- Facilitate **info sharing and technology exchange,** including info security, computer virus and malicious code, among its members;
- Promote **collaborative research and development** on subjects of interest to its members;

Network Security Cooperation

- **Assist other CSIRTs in the region** to conduct efficient and effective computer emergency response capability;
- **Provide inputs and/or recommendations** to help address legal issues related to info security and emergency response across issues regional boundaries;

Emergency Response

- Organize **annual conference** to raise awareness on computer security incident responses and trends.

Computer Security Awareness

APCERT Member Teams

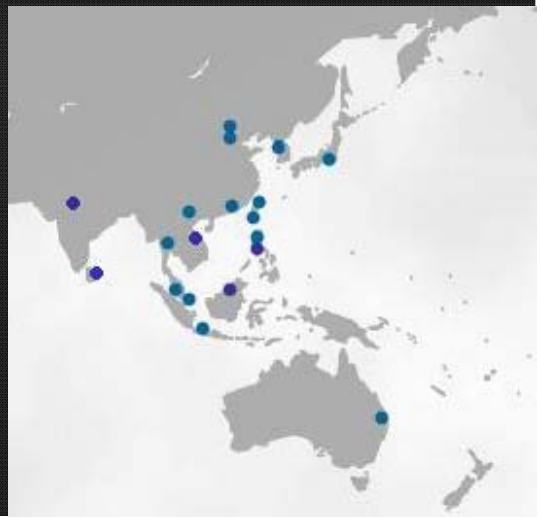
26 Teams/17 Economies, as of Feb 2011
(Started from 15 Teams/12 Economies)

Full Members (18)

- **AusCERT** – *Australia*
- **BKIS** – *Vietnam*
- **BruCERT** – *Negara Brunei Darussalam*
- **CCERT** – *People's Republic of China*
- **CERT-In** – *India*
- **CNCERT/CC** – *People's Republic of China*
- **HKCERT/CC** – *Hong Kong, China*
- **IDCERT** – *Indonesia*
- **JPCERT/CC** – *Japan*
- **KrCERT/CC** – *Korea*
- **MyCERT** – *Malaysia*
- **PHCERT** – *Philippine*
- **SingCERT** – *Singapore*
- **SLCERT** – *Sri Lanka*
- **ThaiCERT** – *Thailand*
- **TWCERT/CC** –*Chinese Taipei*
- **TWNCERT** – *Chinese Taipei*
- **VNCERT** – *Vietnam*

General Members (8)

- **BDCERT** – *Bangladesh*
- **BP DSIRT** – *Singapore*
- **CERT Australia** – *Australia*
- **GCSIRT** – *Philippine*
- **ID-SIRTII** – *Indonesia*
- **MonCIRT** – *Mongolia*
- **NUSCERT** – *Singapore*
- **TechCERT** – *Sri Lanka*



How does APCERT work?

- **CERT (Computer Emergency Response Team)**
  CSIRT (Computer Security Incident Response Team)
  - Independent from politics, industry, market
  - Do not focus on WHO (attribute) and WHY (motivation)
  - Focus on technically what is happening, how to stop the incident, how to prevent it, from a technical coordination perspective

- **CERT/CSIRT Common Policy**
  - My security is depending on your security
  - Web of trust – CSIRT trust relationship is developed based on a long time operation collaboration relationship

- **Systematic Handling – with repeatable procedure, POC agreement**
  - Time manner
  - Each team has appropriate domestic contact to handle / respond to incidents (ISPs, critical infrastructure, government…)
  - Reaching to disconnected areas using CERT/CSIRT network, where it is difficult to reach

Consistent efforts -

- **Developed close collaboration relationship (Bridge the gap)**
  - Regular face to face meetings among teams (Develop trust)
  - Developing long time tactical strategy addressing cyber related incidents
    - Training / Education / Awareness program
  - Daily communication not only incident information but also trends, projects
  - Site visiting time to time, organizing regular gatherings
- **POC arrangement between members**
  - 24 hours Hotline
  - Encrypted communication tool
- **Practice - Incident Handling Drill**
  - Drills organized by APCERT members since 2005
  - ASEAN CERT Incident Drill (ACID) since 2006

Based on operational experience – Outreach to regional communities

- One important role of APCERT is education and training to raise awareness and encourage best practice.
  - APEC-TEL: APCERT provides recommendation / situation awareness / trend to AP regional intergovernmental initiatives as security expert group in AP
  - APCERT received General Guest status at APEC-TEL
  - Other AP regions: APCERT members provide CSIRT trainings and outreach programs to newcomer economies

- Cross regional collaboration
  - TF-CSIRT (TERENA's Task Force of Computer Security Incident Response Teams): European Counterpart of APCERT
  - FIRST: International CERT/CSIRT community

APCERT Annual Events

- **APCERT Drill 2011**
  Date: 22 February 2011
  Participating Teams: 20 teams from 15 economies

- **APCERT AGM& Conference 2011**
  23rd-24th March 2011 in Jeju Island, Korea
  Hosted by KrCERT/CC

23 March (AM)	APCERT Annual General Meeting (AGM) Annual activity reports, future plans, new members, election
23 March (PM)	APCERT Conference (Closed to APCERT members & invited guests)
24 March (All day)	APCERT Conference (Open to public)

- **APCERT Workshop 2011 on TSUBAME Network Traffic Monitoring Project**

25 March (AM)	(Closed to TSUBAME project members)

- *APCERT 2011 Fellowship Program is sponsored by Microsoft*
- *Please find information on the APCERT website (http://www.apcert.org)*

APCERT
Asia Pacific Computer Emergency Response Team

Thank you

APCERT General Contact:

apcert-sec@apcert.org

APCERT Website:

http://www.apcert.org