APCERT Cybersecurity Activities

Asia Pacific Computer Emergency Response Team

Clifton Soh

SingCERT, Singapore
APCERT

AP* Retreat Meeting
24 February 2013

About APCERT

- **A**sia **P**acific **C**omputer **E**mergency **R**esponse **T**eam
  http://www.apcert.org

  - Forum of CSIRTs in the 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 checks based on given scenario
       - In conjunction with local exercise(s)
  - APCERT Annual Report
    http://www.apcert.org/documents/index.html
    - Released every spring
    - Includes APCERT team reports on incident trends, statistics, new projects, and more

APCERT Member Teams

30 Teams / 20 Economies (as of February 2013)
(Started from 15 Teams / 12 Economies)

Full Members (21)

- AusCERT – *Australia (Steering Committee (SC))*
- BKIS – *Vietnam*
- BruCERT – *Negara Brunei Darussalam*
- CCERT – *People's Republic of China*
- CERT Australia – *Australia (SC)*
- CERT-In – *India*
- CNCERT/CC – *People's Republic of China (SC)*
- HKCERT/CC – *Hong Kong, China*
- IDCERT – *Indonesia*
- ID-SIRTII – *Indonesia (SC)*
- JPCERT/CC – *Japan (Chair, SC, Secretariat)*
- KrCERT/CC – *Korea (Deputy Chair, SC)*
- MyCERT – *Malaysia (SC)*
- PHCERT – *Philippine*
- SingCERT – *Singapore*
- Sri Lanka CERT/CC – *Sri Lanka*
- TechCERT – *Sri Lanka (as of March 2012)*
- ThaiCERT – *Thailand*
- TWCERT/CC –*Chinese Taipei*
- TWNCERT – *Chinese Taipei*
- VNCERT – *Vietnam*

General Members (9)

- BDCERT – *Bangladesh*
- BP DSIRT – *Singapore*
- EC-CERT – *Chinese Taipei (as of Aug 2012)*
- GCSIRT – *Philippines*
- MOCERT – *Macau*
- MonCIRT – *Mongolia*
- mmCERT – *Myanmar*
- NCSC – *New Zealand (as of Mar 2012)*
- NUSCERT – *Singapore*

Objectives

APCERT
Asia Pacific Computer Emergency Response Team

- 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 **information 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 security emergency response capability;
- **Provide inputs and/or recommendations** to help address legal issues related to info security and emergency response capabilities across regional boundaries;

Emergency Response

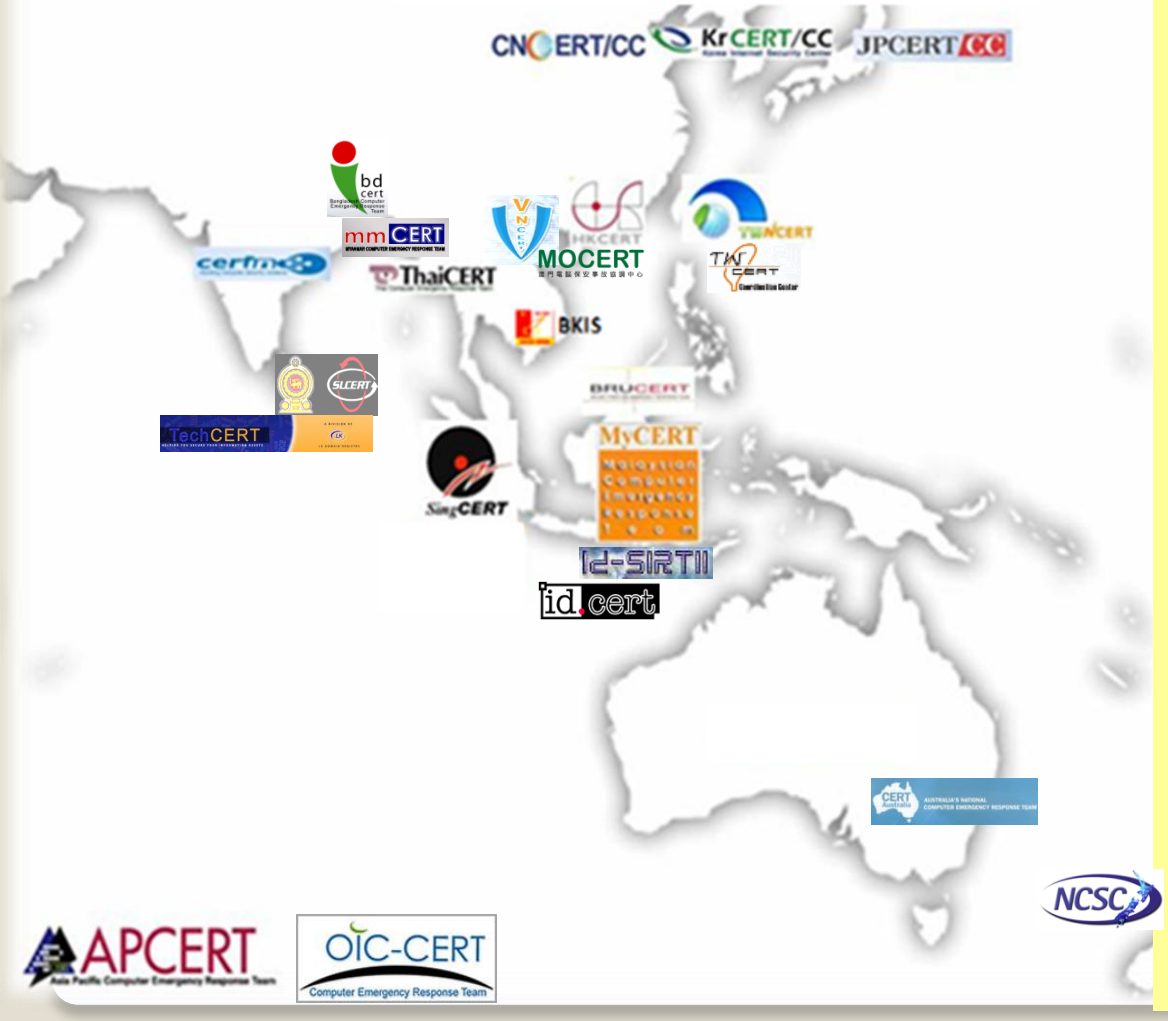
- Organize and conduct an **annual conference** to raise awareness on computer security incident responses and trends.

Computer Security Awareness

APCERT Working Groups

- Information Classification WG
  - ✓To consider appropriate information classification and handling system
  - ✓Convenor: AusCERT
- Information Sharing WG
  - ✓To identify information regarded as useful for APCERT members and/or available to share with other APCERT members
  - ✓Convenor: CNCERT/CC
- Membership WG
  - ✓To review the current membership criteria/classes
  - ✓Convenor: KrCERT/CC
- Operational Framework WG
  - ✓To identify necessary changes to the APCERT Operational Framework
  - ✓Convenor: HKCERT
- TSUBAME WG
  - ✓Internet traffic monitoring project
  - ✓Convenor: JPCERT/CC

APCERT Drill 2013



About the Drill

- **Date: 29 January 2013**

- **Participating Teams:**
22 CSIRTs from 18 economies +
4 CSIRTs from OIC-CERT
(Australia, Bangladesh, Brunei Darussalam, People's Republic of China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Korea, Macao, Malaysia, Myanmar, New Zealand, Singapore, Sri Lanka, Thailand and Vietnam + Egypt, Pakistan, Oman and Tunisia)

- **Theme: "Countering Large Scale Denial of Service Attacks"**

- **Objective/Scenario:** To exercise incident response handling arrangements locally and internationally to mitigate the impact of Denial of Service (DoS) attacks that involved large scale propagation of malicious software acting to impair critical infrastructure and economic activities.

APCERT Study Calls

A knowledge sharing platform for APCERT Teams to exchange technical know-how

1. First APCERT Study Call -
   - Date: 11th July 2012
   - Topic: "Reversing Malicious Flash"
   - Speaker/Organizer: MyCERT, CyberSecurity Malaysia

2. Second APCERT Study Call -
   - Date: 25th January 2013
   - Topic: "Manual malware detection and cleaning"
   - Speaker/Organizer: BKIS (Vietnam)

Recent Achievements/Events (1)

- Joined the 3rd APT Cybersecurity Forum
  - 25-27 September 2012, Macao
  - Introduced APCERT activity updates (MOCERT)
- ASEAN Regional Forum "Cyber Incident Response Workshop"
  - 4-5 September 2012, Singapore
  - Organized by CERT Australia, SingCERT
- APCERT Information Classification Policy
  - APCERT created and published its Information Classification Policy based on the Traffic Light Protocol (TLP) used widely by the international CSIRT community
- APCERT DataExchanger
  - A database is created by CNCERT/CC to share incident related information among APCERT Teams (November 2012)
- APCERT Wiki
  - Officially launched by MyCERT as APCERT's information sharing platform

Recent Achievements/Events (2)

- MoU signed between APCERT – STOP. THINK. CONNECT Messaging Convention (2012)
  - APCERT and the STOP. THINK. CONNECT. Messaging Convention joined forces to propagate the global STOP. THINK. CONNECT. online safety awareness campaign to the 20 economies represented by APCERT's membership.

APCERT 10th Anniversary AGM & Conference 2013 coming!

Theme: "APCERT & Cybersecurity: Then, Now and Beyond"

Date: 24th – 27th March 2013
Venue: Novotel Hotel, Brisbane, Australia
Hosted by: CERT Australia

AP* Retreat colleagues are welcome to join:

25th March (All)	Workshops/Presentations/Panel discussions
26th March (PM)	Closed Conference
27th March (All)	Open Conference

** Note: Through 24th-26th March, there will be some closed meetings exclusively for APCERT members at the same venue, including the APCERT Annual General Meeting (AGM).*

** For registration and further information about the APCERT Conference 2013, please visit our event website (**https://apcert2013.cert.gov.au/**)*

Thank you

APCERT General Contact:
apcert-sec@apcert.org

APCERT Website:
http://www.apcert.org