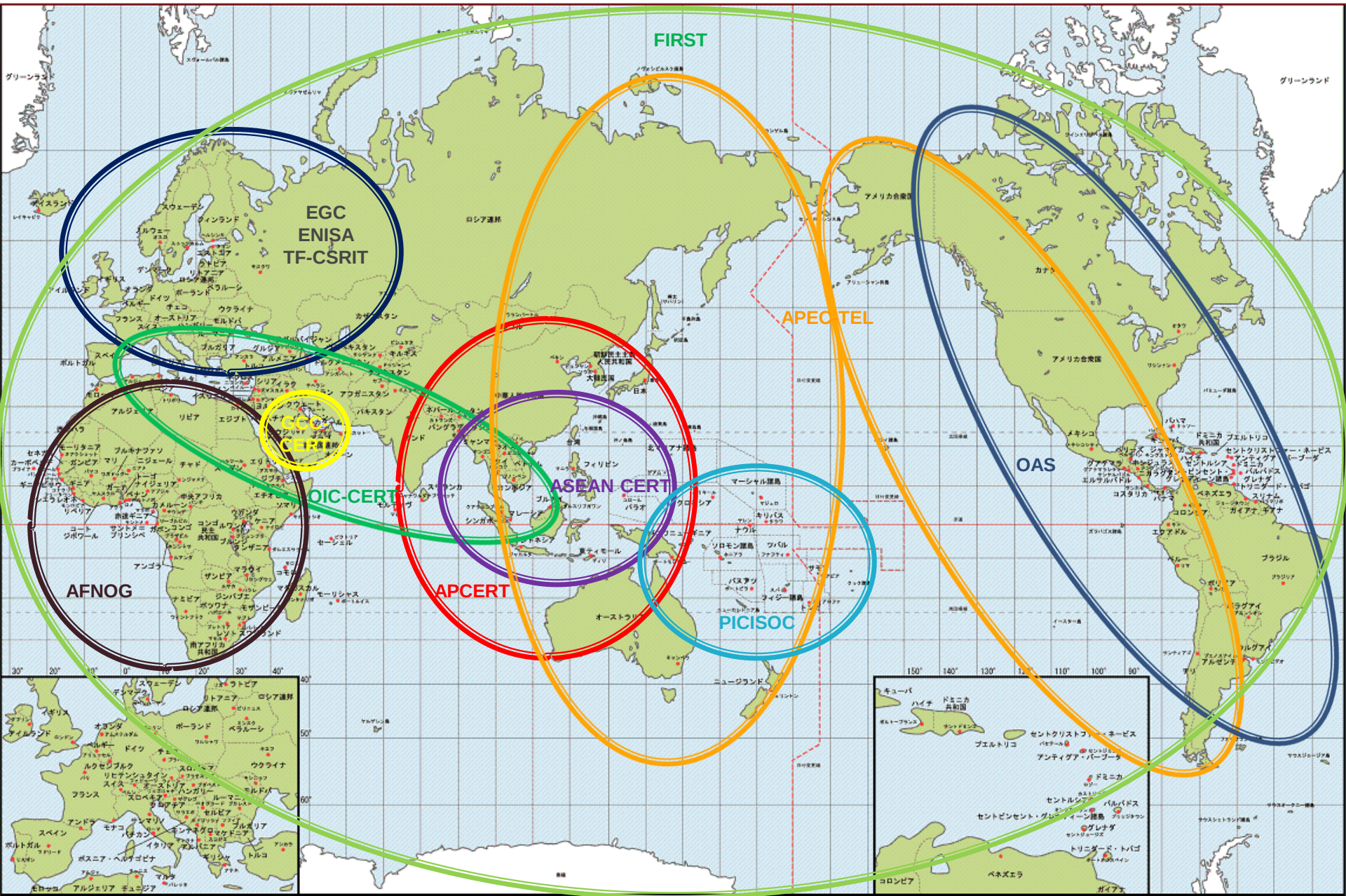
APCERT

Asia Pacific Computer Emergency Response Team Activities & Challenges

Roy Ko
Chair, APCERT
(Centre Manager, HKCERT)

CERT/CSIRT Regional Communities in the World

APCERT
Asia Pacific Computer Emergency Response Team



About APCERT

- Asia Pacific Computer Emergency Response Team
  http://www.apcert.org
  - Forum of CSIRTs in AP region
  - Established in February 2003
  - Annual Events
    - APCERT Annual Conference
      - Sharing latest activities, trends, challenges, discussions on international collaboration, etc.
    - APCERT Drill

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;

- 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;

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

Network Security Cooperation

Emergency Response

Computer Security Awareness

APCERT Member Teams

23 Teams/16 Economies, as of August 2009

Full Members (17)

- AusCERT – *Australia*
- BKIS – *Vietnam*
- CCERT – *People's Republic of China*
- CERT-In – *India*
- CNCERT/CC – *People's Republic of China*
- HKCERT – *Hong Kong, China*
- IDCERT – *Indonesia*
- JPCERT/CC – *Japan*
- KrCERT/CC – *Korea*
- MyCERT – *Malaysia*
- PHCERT – *Philippine*
- SingCERT – *Singapore*
- SLCERT – *Sri Lanka – New! (March 2009)*
- ThaiCERT – *Thailand*
- TWCERT/CC –*Chinese Taipei*
- TWNCERT – *Chinese Taipei*
- VNCERT – *Vietnam*

General Members (6)

- BDCERT – *Bangladesh*
- BP DSIRT – *Singapore*
- BruCERT – *Negara Brunei Darussalam*
- GCSIRT – *Philippine*
- ID-SIRTII – *Indonesia – NEW! (June 2009)*
- NUSCERT – *Singapore*

APCERT Drill 2007

- Date : 22nd December 2007
- Participation teams:
  - Malaysia – MyCERT
  - Australia – AusCERT
  - Brunei – BruCERT
  - China – CNCERT
  - Singapore – SingCERT
  - Thailand – ThaiCERT
  - Hong Kong – HKCERT
  - India – CERT-In
  - Japan – JPCERT
  - Korea – KRCERT
  - Chinese Taipei – TWNCERT
  - Vietnam –BKIS

Timeline

- **0700** Lord of Armageddon (LoA) declare cyber war on Beijing Olympics
- **0900** Co-ordinated botnet attacks from AP region causing media sites and government portals inaccessible
- **1100** Spam containing malware that turns PC into zombies were filling up mailboxes in AP economies
- **1300** Border and Core routers crashing and rebooting frequently. 0-day exploit for Cisco IOS rumoured to be available. Cisco promise to release fix in a few hours
- **1430** – Cisco released patch and advisory on critical IOS vulnerability
- **1600** – Security analysts announced that bots automagically removed themselves, no more attacks

APCERT Drill 2008

- **Date: 4th December 2008**
- **14 Participant Teams**

AusCERT
BKIS
BruCERT
CERT-In
CNCERT/CC
HKCERT
JPCERT/CC
KrCERT/CC
MyCERT
SingCERT
TWNCERT
ThaiCERT
SLCERT
VNCERT

Drill Scenario

- Scenario:
  A massive cyber attack by organized criminals engaging in data theft and illegal online services.
- Objective:
  Improve timely technical response and decision making/coordination procedures
- Across 5 time zones
  9 hour drill

Awareness Raising

- Target – Security incident response communities, security experts, policy makers

- APCERT Annual Conference
  - Exchange views with security experts of Asia Pacific CSIRTs and other closely related organizations
  - Local outreach to critical entities and local government

- APCERT Drill
  - Annual communication check drill based on the scenario
  - In conjunction with local exercises
  - Promotion video

- Liaison Activities
  - FIRST, TF-CSIRT, GCC, OAS, AFNOG, APEC-TEL, ASEAN, ICANN, APNIC, DotAsia, ITU, APWG, AP*…

- APCERT Annual Report
  - Member teams report on incident trends, statistics, new projects, etc.
  - http://www.apcert.org/documents/index.html

APCERT at Regional Events

- AVAR 2008, 10th–12th December 2008 in New Delhi, India
  - APCERT contributed as Supporting Partner of the event.
  - http://www.aavar.org/avar2008/index.htm
- OIC-CERT Seminar 2009 for OIC Countries 13th–15th January 2009 in Kuala Lumpur, Malaysia
  - CyberSecurity Malaysia organized the seminar
- APEC TEL 39, 13th–18th April 2009 in Singapore
  - APCERT collaborative responses on Conficker Worm (APCERT Chair – HKCERT)
  - APCERT Cyber Drill Exercise 2008 (MyCERT)
  - TSUBAME Network Monitoring Project (JPCERT/CC)
- FIRST Annual Conference 2009, 28th June – 3rd July 2009 in Kyoto, Japan
  - APCERT Meeting & Dinner

Collaborative Responses on Conficker Worm

APCERT

- List of machines infected by Conficker.C
  - Teams endeavored to contact victims
- Worm sample
  - Reverse engineering the code
- Analysis results
  - Domain names generated
- Handling Strategy
  - Sinkholes to capture activities of the worm
- Other researches published

Other Collaborative Initiatives

- Conficker Working Group
- Microsoft Bounty of US $250,000
- ICANN & Domain Name Registries, Law Enforcement, ISPs
- Message to the general public
  - No major outbreak, but emerging threat

Other Activities & Affiliations

- **Visiting New CSIRTs in Asia Pacific**
  - APCERT SC members visited several CSIRTs and relevant government departments, to support and cooperate in incident handling and information sharing
- **APEC TEL General Guest**
  - APCERT provides recommendations, situation awareness and trends to APEC intergovernmental initiatives, as security experts in the AP region
- **DotAsia Advisory Council Member**
  - APCERT assists DotAsia in policy development and relevant community projects

Upcoming Activities

Looking Forward

- APCERT Drill 2009
- APCERT Annual Conference 2010
  - 3rd–5th March 2010 in Phuket, Thailand
  - Annual General Meeting
    New Members, Annual Reports, Election, Future Developments
  - Conference & Workshop

Thank you

APCERT General Contact:
apcert-sec@apcert.org

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