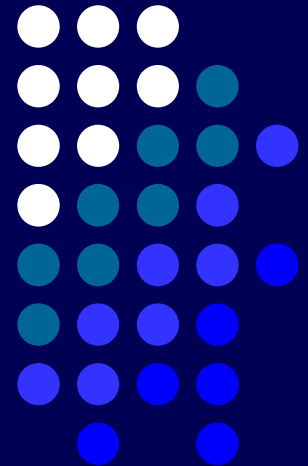
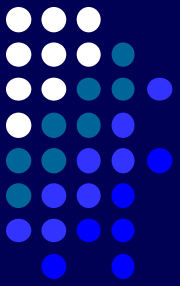


# APCERT Updates

*Asia Pacific Computer Emergency Response Team*

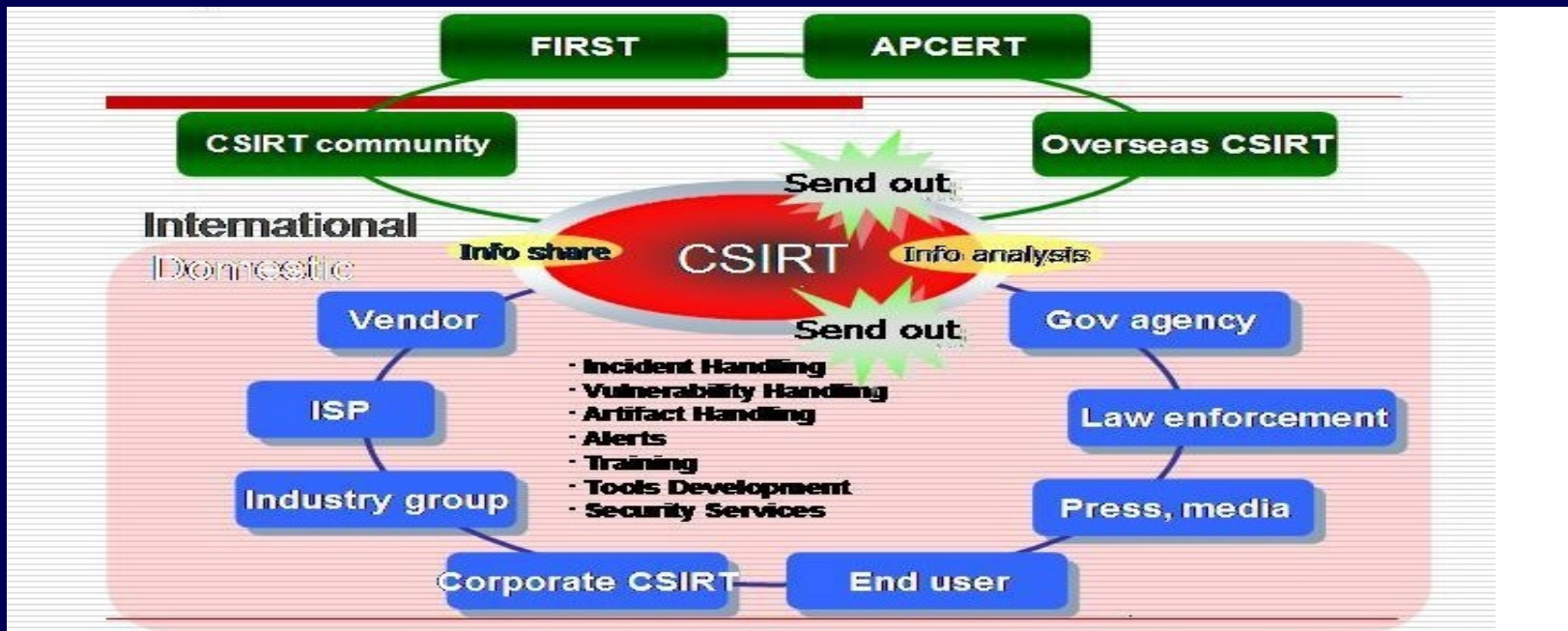
**Megat Muazzam Abdul Mutalib**  
**Intrusion Analyst, MyCERT**  
*On behalf of APCERT*

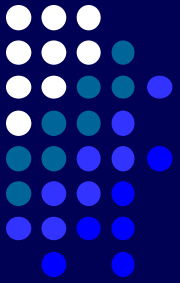




# About APCERT & CSIRT

- APCERT (Asia Pacific CERT) is a coalition of the forum of CSIRTs\* . (*CSIRT: Computer Security Incident Response Team*)
- Open to all suitably qualified CERTs and CSIRTs in the Asia Pacific region.
- To improve the region's awareness and competency in relation to computer security





# APCERT Member Teams

**21 Teams from 15 Economies, as of 11<sup>th</sup> March 2008**

## Full Members (14)

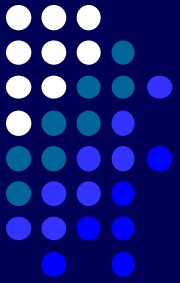
- **AusCERT** – *Australia*
- **BKIS** – *Vietnam*
- **CCERT** – *People's Republic of China*
- **CNCERT/ICC** – *People's Republic of China*
- **HKCERT/ICC** – *Hong Kong, China*
- **IDCERT** – *Indonesia*
- **JPCERT/ICC** – *Japan*
- **KrCERT/ICC** – *Korea*
- **MyCERT** – *Malaysia*
- **PH-CERT** – *Philippine*
- **SingCERT** – *Singapore*
- **ThaiCERT** – *Thailand*
- **TWCERT/ICC** – *Chinese Taipei*
- **TWNCERT** – *Chinese Taipei*

## General Members (7)

- **BP DSIRT** – *Singapore*
- **BruCERT** – *Negara Brunei Darussalam*
- **CERT-In** – *India*
- **GCSIRT** – *Philippine*
- **NUSCERT** – *Singapore*
- **VNCERT** – *Vietnam*
- **SLCERT** – *Sri Lanka*



# 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.



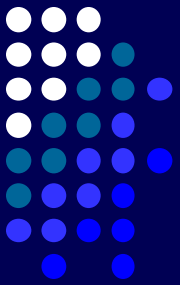
**Network Security  
Cooperation**



**Emergency  
Response**

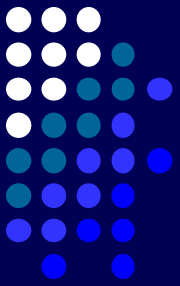


**Computer Security  
Awareness**



# ***APCERT Activity Updates 1***

- **PacINET 2007, 14-22 August 2007, Solomon Islands**  
*<http://www.picisoc.org/tiki-index.php?page=PacInet+2007>*
  - **AusCERT interacted with Pacific Islanders', who are willing to start discussions about CERT capability developments.**
- **ITU Regional Workshop, 28-31 August 2007, Hanoi, Vietnam**  
*<http://www.itu.int/ITU-D/cyb/events/2007/hanoi/>*
  - **MyCERT, AusCERT, CNCERT/CC, JPCERT/CC attended the "Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection".**
  - **Indonesia and Mongolia are also willing to discuss CERT capability developments.**



# APCERT Activity Updates 2

- **APEC TEL 36, 21-26 October 2007, Santiago, Chile**

[http://www.apectel36.cl/prontus\\_apectel/site/edic/base/port/home.html](http://www.apectel36.cl/prontus_apectel/site/edic/base/port/home.html)

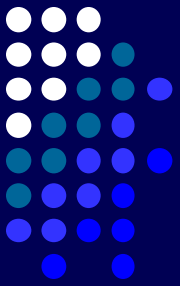
- CNCERT/CC, JPCERT/CC, KrCERT/CC, MyCERT attended the “Workshop on Cyber Security Exercises” and shared experience of the APCERT Incident Handling Drill.
- CNCERT/CC is forwarding a project on “Guide on Policy and Technical Approaches Against Botnets”.

\* As a Security Expert Group, APCERT provides recommendation, situation awareness and trend to AP regional intergovernmental initiatives. APCERT is a General Guest of APEC TEL.

- **5-9 November 2007, Miami, USA**

[http://www.cicte.oas.org/Rev/EN/Events/Cyber\\_Events/II\\_Workshop\\_MIAMI-2007](http://www.cicte.oas.org/Rev/EN/Events/Cyber_Events/II_Workshop_MIAMI-2007)

- MyCERT attended and had interactions with OAS (Organization of American States) and APWG (Anti-Phishing Working Group).



# ***APCERT Activity Updates 3***

- **APCERT Drill 2007, 22 November 2007**

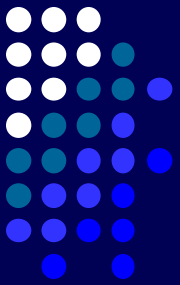
<http://www.apcert.org/documents/pdf/APCERT-drill-2007.pdf>

- The drill was to reinforced the collaboration and communication between APCERT teams
- The event was reinvented to take on the scenario of an attack during the Beijing 2008 Olympic Games

- **APCERT AGM & Conference 2008, 10-12 March 2008**

<http://apcert2008.hkcert.org/>

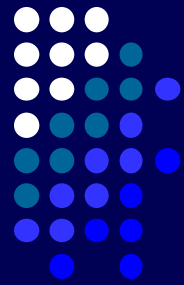
- The 7<sup>th</sup> APCERT Annual Conference, provides an opportunity for APCERT Teams, CSIRTs of the AP region, and other closely related organizations to come together and share different experiences, perspectives and best practices on information security.



# *Other APCERT Updates*

- 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.
- Other International Relationships & Engagements
  - FIRST Director & SC Member: Ms. Yurie Ito, JPCERT/CC
  - APEC TEL SPSG Conveyor: Mr. Jinhyun Cho, KrCERT/CC
- IRC communication
  - An IRC server is to be operated for teams to improve communication between teams in 2008
    - Not used as an Incident handling means
- APCERT Drill 2008
  - To be around end of the year.

# APCERT DRILL 2007 (1)



Date: 22<sup>nd</sup> November 2007

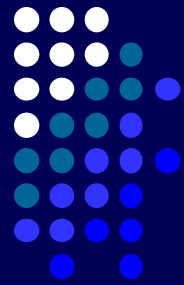
Participating teams:

- Malaysia – MyCERT
- Australia – AusCERT
- Brunei – BruCERT
- China – CNCERT
- Singapore – SingCERT
- Thailand – ThaiCERT
- Hong Kong – HKCERT
- India – CERT-In
- Japan – JPCERT
- South Korea – KRCERT
- Chinese Taipei – TWNCERT
- Vietnam – BKIS

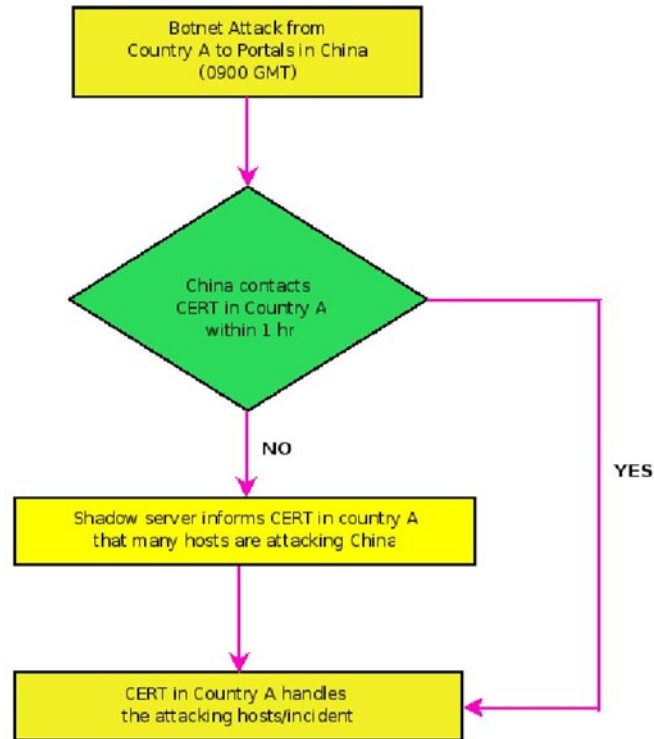
## Timeline

- ♦ **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 automatically removed themselves, no more attacks

# APCERT DRILL 2007 (2)



## Scenario Handling



# Thank you

**APCERT General Contact:**

**[apcert-sec@apcert.org](mailto:apcert-sec@apcert.org)**

**APCERT Website:**

**<http://www.apcert.org>**

