Introduction of APCERT

Yurie Ito, JPCERT/CC

(On behalf of the APCERT Secretariat)

APCERT

- **APCERT** *(Asia Pacific Computer Emergency Response Team)* is a coalition of the forum of CSIRTs *(Computer Security Incident Response Teams)*. The organization was established to encourage and support the activity of CSIRTs in the Asia Pacific region.
- Started from 15 teams from 12 economies

→ Now 17 teams from 13 economies

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 CERTs and 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 regional boundaries,
- Organize an annual conference (APSIRC) to raise awareness on computer security incident responses and trends.

Members

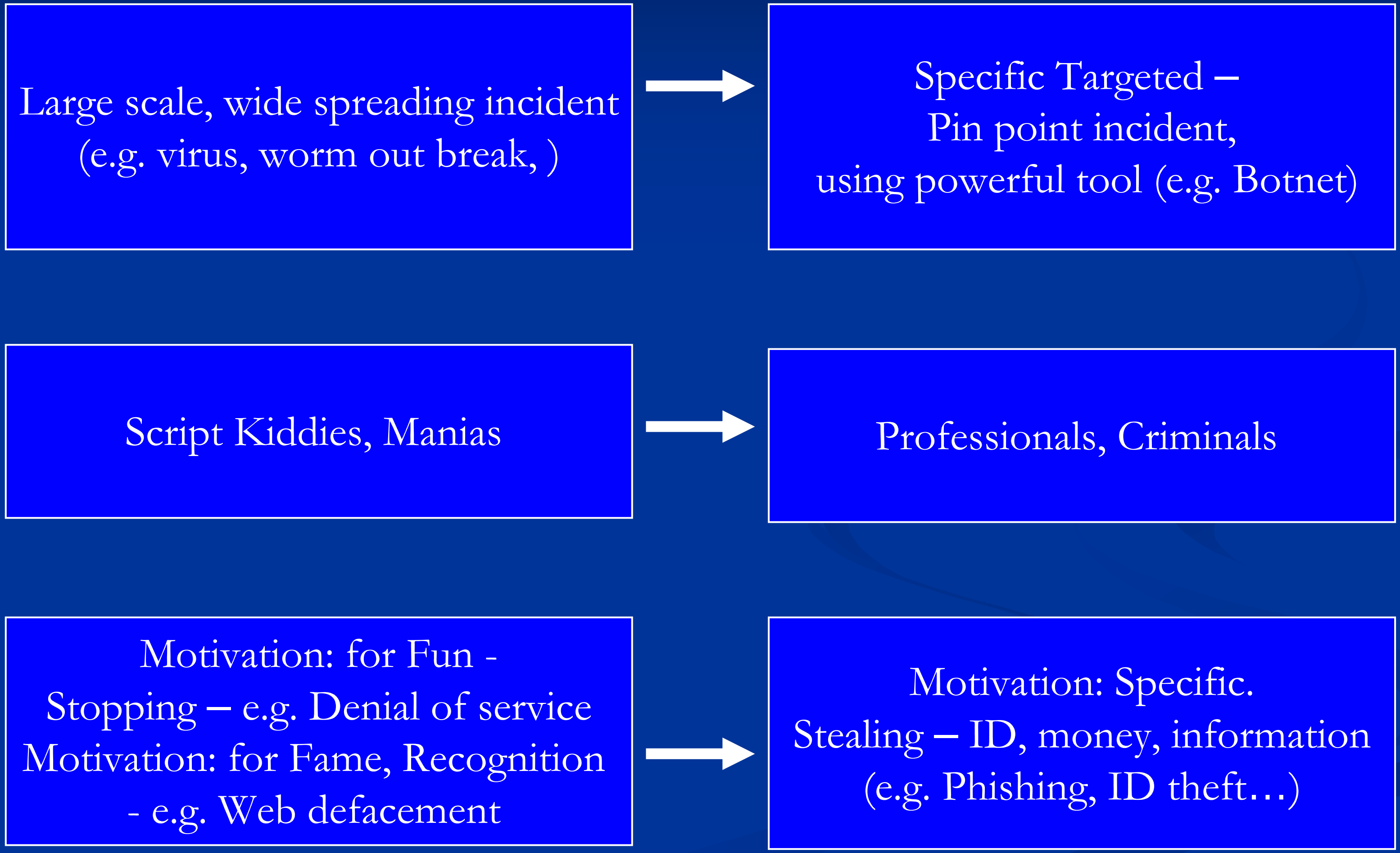
Full Members (15)

- **AusCERT** (Australian Computer Emergency Response Team) – *Australia*
- **BKIS** (Bach Khoa Internetwork Security Center) – *Vietnam*
- **CCERT** (CERNET Computer Emergency Response Team) – *People's Republic of China*
- **CNCERT/CC** (National Computer network Emergency Response technical Team / Coordination Center of China) – *People's Republic of China*
- **HKCERT/CC** (Hong Kong Computer Emergency Response Team Coordination Center) – *Hong Kong, China*
- **IDCERT** (Indonesia Computer Emergency Response Team) – *Indonesia*
- **JPCERT/CC** (Japan Computer Emergency Response Team / Coordination Center) – *Japan*
- **KrCERT/CC**(Korea Computer Emergency Response Team Coordination Center, Korea Internet Security Center, KISA) – *Korea*
- **MyCERT** (Malaysian Computer Emergency Response Team) – *Malaysia*
- **PH-CERT** (Philippine Computer Emergency Response Team) – *Philippine*
- **SecurityMap.Net CERT** (Securitymap Networks Computer Emergency Response Center) – *Korea*
- **SingCERT** (Singapore Computer Emergency Response Team) – *Singapore*
- **ThaiCERT** (Thai Computer Emergency Response Team) – *Thailand*
- **TWCERT/CC** (Taiwan Computer Emergency Response Team / Coordination Center) – *Chinese Taipei*
- **TWNCERT** (Taiwan National Computer Emergency Response Team) – *Chinese Taipei*

General Members (2)

- **BruCERT** (Brunei Computer Emergency Response Team) – *Negara Brunei Darussalam*
- **GCSIRT** (Government Computer Security and Incident Response Team) – *Philippine*

Cyber security Incident is changing



Large scale, wide spreading incident
(e.g. virus, worm out break,)

→

Specific Targeted –
Pin point incident,
using powerful tool (e.g. Botnet)

Script Kiddies, Manias

→

Professionals, Criminals

Motivation: for Fun -
Stopping – e.g. Denial of service
Motivation: for Fame, Recognition
- e.g. Web defacement

→

Motivation: Specific.
Stealing – ID, money, information
(e.g. Phishing, ID theft…)

Incident Handling among members is changing

- Start handling more complicating incidents

- 2002-2003 (when APCERT was formed)
  - Response to the Wide-spreading Incident
    - Slammer incident response case
  - Reporting network traffic flow, updating local activities
  - Sharing technical information and vendor's notes

- 2004-2005 (recent incident response)
  - Response to the "Specific Targeted" – pin point attack
  - Members sharing info

e.g. public monitoring information attack announcement, targeted site, attacking tool information to help each team to protect constituency

- Recent China – Japan –Korea collaboration case
- Phishing site coordination

How does APCERT work ?

- CSIRT Computer Security Incident Response Team's incident response
  - Independent from politics, market, industry
  - 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 technical perspective coordination

- 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
  - Timely manner
  - Each teams has appropriate domestic contacts to handle/response incidents. (ISPs, critical infrastructure, government…)
  - Reaching to disconnected place using CSIRT network, where is difficult to reach

- Consistent efforts

- Developed close collaborating relationship (Bridge the gap)
  - Regular face to face meetings between teams (Develop trust)
  - Developing long time tactical strategy addressing cyber related issues and work together -
    - Training/Education/Awareness program
  - Daily communication not only incident information but about team structure, problem, trend, project
  - Site visiting time to time, Organizing regular gatherings

- POC arrangement between members
  - 24 hours Hotline
  - encrypted communication tool

- Practice - incident handling exercise
  - CJK exercise 2004, expand the drill to all members

Based on operational experience – Outreach to multiple sectors

- One important role of APCERT is education and training to raise awareness and encourage best practice.
  - APEC-TEL: APCERT provided the recommendation/ situation awareness / trend to AP regional intergovernmental initiative as security experts group in AP
  - APCERT got the General Guest status at APEC-TEL
  - ASEAN: APCERT members provide CSIRT training and Outreach program to newcomer economies

- Cross regional collaboration
  - TF-CSIRT (TERENA's Task Force of Computer Security Incident Response Teams): European Counterpart of APCERT
  - FIRST: Implement "TRANSITS" standard CSIRT training material, add regional modules on top of the core material.
    - TRANSITS program – from EU

Thank you.

- APCERT general contact (apcert-sec@apcert.org)
- http://www.apcert.org

- Yurie Ito (yito@jpcert.or.jp)
  - Director, Technical Operation, JPCERT/CC
- Tel: 81-3-3518-4600