APCERT Updates

Asia Pacific Computer Emergency Response Team Activities & Challenges

Adli Wahid <adli@cybersecurity.my>
MyCERT
SC member of APCERT

AP* Retreat, Kuala Lumpur
28th February 2010

About APCERT

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

  - Forum of CERTs/CSIRTs in AP region
  - Established in February 2003
  - Annual Events
    1. APCERT Annual Event
       - Exchange security trends & challenges among experts
       - Local outreach and awareness raising for local government & critical entities
    2. APCERT Drill (Cyber attack exercise)
       - Communication check drill based on scenario
       - In conjunction with local exercise

- APCERT Annual Report <http://www.apcert.org/documents/index.html>
  - Member 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

23 Teams/16 Economies, as of Feb 2010 (No update – few teams in process)

Full Members (17)

- **AusCERT** – *Australia*
- **BKIS** – *Vietnam*
- **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 (6)

- **BDCERT** – *Bangladesh*
- **BP DSIRT** – *Singapore*
- **BruCERT** – *Negara Brunei Darussalam*
- **GCSIRT** – *Philippine*
- **ID-SIRTII** – *Indonesia*
- **NUSCERT** – *Singapore*

APCERT Drill 2010

About the Drill

- **Date: 28 January 2010**

- **Participating Teams: 16 teams/14 economies**
  (Australia, Brunei, China, Chinese Taipei, Hong Kong China, India, Indonesia, Japan, Korea, Malaysia, Singapore, Sri Lanka, Thailand, Vietnam)

- **Theme: "Fighting Cyber Crimes with Financial Incentives"**

- **Scenario:** Financial web sites (ex. e-banking, e-auction, stock trading) under several attacks by cyber criminals, aiming to paralyze online business activities, compromise user credentials and to transfer money to fuel the underground economy.

- **Objective:** Exercise incident response handling operations locally and internationally to mitigate the impact of ongoing attacks and to improve the coordination capability.

APCERT at Regional Events

- **APEC TEL 40** (Sep 2009 - Mexico)
  - **Presentations:**
    - **APCERT activities, education/awareness efforts and outreach programs**
- **AVAR2009** (Nov 2009 - Japan)
  - **APCERT contributed as Supporting Partner**
  - **AVAR 2009 – 12th Association of anti-Virus Researchers International Conference, the leading anti malware conference in the Asia-Pacific region**
- **FIRST Technical Colloquium** (Dec 2009 - Malaysia)
  - **CyberSecurity Malaysia and Team Cymru co-hosted the FIRST Technical Colloquium**
- **2nd PacCERT Working Group Meeting** (Feb 2010 - Fiji)
  - **Pacific regional CERT (PacCERT) is being established by the efforts of ITU, Department of Broadband, Communications and the Digital Economy (DBCDE), Australian Government, AusCERT, APCERT and others.**

Member teams local programs

- **AusCERT**
  - Provides and hosts "Stay Smart Online Alert Service" for the Australian Government - a free subscription based service that provides home users and small to medium enterprises with information on latest computer network threats, vulnerabilities, solutions to help manage the risks, in simple, non-technical, easy to understand language.
    Stay Smart Online: http://www.staysmartonline.gov.au/
  - Performed a scoping study to ascertain the readiness of Pacific Island nations to establish a regional Pacific Island CERT capability (Sponsored by the Australian Government and ITU).
    The report is available at:

    http://www.itu.int/ITU-D/asp/CMS/Events/2009/PacMinForum/doc/Interim_PacificCERT_Readiness_Assessment_(AusCERT).pdf
  - In conjunction with local information security groups, AusCERT hosts a free, yearly 'Computer Security Day' (an international event to raise the awareness of computer security issues) seminar to which IT professionals are invited, for the opportunity to hear noted speakers in the area of IT security - http://www.auscert.org.au/csd
  - External security bulletins and other documents published by AusCERT are freely available via a searchable interface at the AusCERT web site - http://www.auscert.org.au

Member teams local programs

- **BDCERT**
  - Training / Workshop
    - BDCERT team participate in the seminar on "Cyber Crime: Investigation Perspective" organized jointly by Bangladesh Police and Information Technology Management Association of Bangladesh (ITMAB) on 27th & 28th June 2009. Mr. N. B. K. Tripura NDC, Additional Inspector General, Bangladesh Police was the chief guest of the seminar. All the high officials of Bangladesh Police attended the seminar.
  - Publication
    - BDCERT publish an article "Evolution of Cooperation in Cyber Security & BDCERT Activities" in "Digital March 2009" published by ISPAB (Internet Service Provider Association, Bangladesh); supported by BTRC (Bangladesh Telecommunication Regulatory Commission) & IBPC (ICT Business Promotion Council), Ministry of Commerce on the event of World Telecommunication and Information Society Day (WTISD).
  - Awareness Program
    - As a part of awareness program, BDCRT publish "Safety Tips on Internet Chat" in "Digital March 2009" magazine.
    - BDCERT send several alters on Security Update of Conficker.C worm.
    - BDCERT also has awareness programs regularly published in the IT Magazines.
    - BDCERT participate in WTISD Awareness Program on Computer Security. 1000 Students of 7 different schools participate in this program.

Member teams local programs

- **BKIS**
  - Training
    - Network Security Training Courses:
      - June 2009: For Engineers of Ministry of Public Security
      - June 2009: For Network Administrators from companies (Banks, Securities...)
    - Security Awareness Training Courses:
      - July and September 2009: 6 classes for BaoViet Finance Insurance Group
  - Security Advisories
    - In the end of 2008 and 2009, BKIS has discovered and published 19 advisories of software vulnerabilities.
    - http://security.bkis.vn/

Member teams local programs

- **CNCERT/CC**
  - Guide on Policy and Technical Approaches against Botnet, drafted by CNCERT, was published on APEC Website on Dec. 2008.
  - China-ASEAN Network Security Seminar, which was sponsored by the MIIT and hosted by CNCERT, was held in Shenzhen, April 2008.

Member teams local programs

- **HKCERT**
  - Working with Police and Government in an annul program called the Hong Kong Clean PC Day.
    - This year the program involves several quarterly public awareness seminars.
  - Holding an online story writing competition for higher school students with theme "online e-commerce security"
  - Held an ISP Symposium for security awareness promotion with service providers
  - Held a local drill with some ISPs and domain name registries (.hk and .asia)
  - Visiting several partners' offices, discussing closer collaboration

Member teams local programs

- **JPCERT/CC**
  - Leading the APCERT TSUBAME WG
    - Internet Traffic Monitoring Data Visualization Project in Asia Pacific region
  - Supporting the establishment/operations of newer CERT/CSIRTs in the region
    - Cambodia, Mongolia, Lao PDR, Pacific Islands
    - Together with Japanese organizations – JICA, CICC
  - Conducted IT security seminars/workshops/trainings in local events
    - Vietnam, Indonesia, Sri Lanka
  - Conducted C/C++ Secure Coding Seminar
    - Thailand, Indonesia, Vietnam
  - CCC (Cyber Clean Center) – AntiBot Project
    - https://www.ccc.go.jp/en_index.html
  - Started Security Alerts & Vulnerability Notes in English
    - http://www.jpcert.or.jp/english/

Member teams local programs

- **MyCERT**
  - Training
    - Incident Handling Training for Egypt CERT and Oman CERT
    - Various local training on malware analysis and web security
  - Speaking engagements at various events such as:
    - FIRST Annual Conference in Kyoto
    - APWG Counter E-Crime Conference in Barcelona
    - Annual Honeynet Project Meeting
  - Launching of Cyber999 and Malware Research Centre
  - Incident handling (Cyber999) service and security alerts publication at http://www.mycert.org.my
  - General awareness @ http://www.cybersafe.my

Member teams local programs

- **SingCERT**
  - Incident Drill
    - SingCERT planned and co-ordinated the 4th ASEAN CERT Incident Drill in Jul 09. In total, 14 CERTs from 12 countries took part in the drill.
    - The drill was successful in meeting its objectives to enhance the incident investigation and co-ordination between CERTs in the area of tracking and bringing down Botnet. All participating teams unanimously agreed that it was a successful drill, both engaging and challenging.
  - Visits
    - Hosted visit by representatives from Kenya and Tanzania to discuss setup of national CERTs
    - Hosted visit by Oman CERT

Member teams local programs

SLCERT

- Knowledge sharing session on Latest Information Security trends
  - This was organized by SLCERT and conducted by a Threat Intelligence Engineer from idefence Labs, USA.
  - The target audience was CEOs, Engineers and IT Managers.
- Public awareness campaign on information security in "Deyata Kirula" exhibition
  - This is a major national Independence Day exhibition in Sri Lanka and SLCERT had the opportunity to run an awareness programme to make the general public including home users and students aware of IS threats and vulnerabilities and how to overcome them.
- Presentation on Managed Security Services for Public & Private sector organizations to guide them on how to manage information security more easily
  - SLCERT organized this with a consultant of Managed Security Services, to give a broad idea about this area to top management of major companies in Sri Lanka.
- Presentation in Chief Innovative Officer's Conference on "Information Security"
  - SLCERT addressed the CIO's highlighting the importance of implementing security requirements on their respective organizations.
- Lecture for MBA Students on "Information Security for E-Governance"
  - This was conducted by SLCERT to raise the awareness on IS to these students as part of their course curriculum.
- Public awareness presentation on "Information Security" at University of Moratuwa
  - SLCERT educated the general public on IS in an event organized by University of Moratuwa.
- CSW-2009 (Computer Security Week- 2009) Conference and workshops
  - This is a major annual event organized by SLCERT. This year SLCERT conducted two workshops;
    - 1. Network and web application security
    - 2. Malware analysis
  - The two-day conference consisted with 16 presentations covering different areas of IS and with large gathering. Several International speakers from JPCERT/CC, Microsoft etc. contributed a lot to make this event success.
- Published 6 critical alerts on SLCERT web site
  - http://www.slcert.gov.lk/AlertsList.php
  - SLCERT have published very critical IS alerts based on their relevancy to our constituency. These alerts have been sent to our subscribers as well.

Member teams local programs

- **ThaiCERT**
  - ThaiCERT staff was invited speaker for:
    - "Incident cases, policies, issues and concerns (tentative)", Sofitel Centara Grand Bangkok (Ladprao), Bangkok, Thailand
    - "Web Security - Hands on", Khon Kaen University, Khon Kaen, Thailand
    - "Security Awareness Raising", Net ProtEX 2009, Swissotel Le Concorde Hotel, Bangkok, Thailand
    - "Security Attack Trends", IDC's Asia/Pacific SecurityVision Conference 2009, The Westin Grande Sukhumvit, Bangkok, Thailand
    - "Cyber Threats", Information Security Training and Awareness Raising Seminar, Vientien, Lao PDR
    - "Introduction to Malware", Suan Kularb High school, Bangkok, Thailand
    - "IT Mananagement and Security Awareness", Thammasart University, Pathumthani, Thailand
  - ThaiCERT organized the seminar:
    - September 1st - 4th, 2009, "C/C++ Secure Coding Essential", Thailand Science Park, Pathumthani, Thailand
  - Publication in Thai language at http://www.thaicert.org
    - Virus alert 1 article (W32.Conficker.C)
    - CERT Advisories 19 articles
    - Documents 3 articles

Member teams local programs

- **TWNCERT**
  - 2009 Information Security Contest (includes Catch-the-Flag, Slogan, Poster and Animation Contest) starts from 2009/9
  - 12 Governmental Information Security Conferences:
    - 2009/3 and 2009/7
  - 5 Email Social Engineering Workshops:
    - TrackRUSE System Introduction: 2009/6
  - 3 Information Security Internal Audit Trainings:
    - 2009/8
  - Website: Information Security Legal Case Study per Month

UPCOMING ACTIVITIES

Looking Forward

- **APCERT AGM & Conference 2010**
  http://apcert2010.thaicert.org/
  - **3rd-4th March 2010 in Phuket, Thailand**

    1. APCERT AGM
    New Members, Annual Reports, Election, Future Developments

    2. Conference
    Invited guests & local information security professionals

    3. TSUBAME Workshop
    Workshop on Internet Traffic Monitoring Data Visualization Project in conjunction w/APCERT AGM & Conference

  - **Fellowship sponsored by Microsoft**

Thank you

APCERT General Contact:

apcert-sec@apcert.org

APCERT Website:

http://www.apcert.org