APCERT
Asia Pacific Computer Emergency Response Team

Activities, Challenges & Collaboration

TLP: WHITE

Prepared by
APCERT Secretariat

February 2018
About APCERT

- **Asia Pacific Computer Emergency Response Team**
  - [http://www.apcert.org](http://www.apcert.org)
  - Forum of CSIRTs/CERTs in the Asia Pacific region
  - Established in February 2003
  - 30 Operational Members from 21 economies
    - New members: Bhutan (BtCIRT), CERT NZ
- APCERT also has MOU/cooperative relationships with
  - STOP.THINK.CONNECT
  - TF-CSIRT (CSIRT community in Europe)
  - OIC-CERT (Organisation of Islamic Cooperation CERT)
  - APNIC

**APCERT Vision Statement**

APCERT will work to help create a **Safe, Clean and Reliable** cyber space in the Asia Pacific Region through global collaboration.
APCERT’s Outreach
- Cross regional collaboration
APCERT Operational Members
(30 Teams from 21 Economies)

Corporate Partners (3)
- Bkav (Vietnam), Microsoft, Secureworks

Japanese
- JPCERT/CC

South Korean
- KrCERT/CC

Taiwanese
- TWCERT/CC, EC-CERT

Vietnamese
- VNCERT

Bruneian
- BruCERT

Indonesian
- ID-SIRTII/CC, ID-CERT

Australian
- AusCERT

New Zealand
- CERT NZ

Copyright © 2018 APCERT
APCERT OM Criteria

1. be a **CERT from an Asia Pacific economy**, which performs the function of a CSIRT or CERT on a full time basis
2. be a **leading or national CERT** within its own economy
3. be **not-for-profit** and/or wholly or partly government funded
4. have **established policies, practices and procedures** for operating a CERT within its economy and have **experience in CERT operations** including incident handling and cyber threat and vulnerability monitoring and advice
5. have a broad **responsibility and capability for disseminating information and coordinating incident response** across and/or among sectors within its economy
6. Obtain an OM sponsor, application and site visit
Asia-Pacific Region

Source: APNIC
APCERT Membership

Are you a CERT/CSIRT or other cyber security or Internet related organisation seeking to join or partner with APCERT?

Yes

Are you a CERT/CSIRT that is not-for-profit and/or wholly or partly government funded?

Yes

Are you located in the Asia-Pacific region (as defined by APNIC)?

Yes

Do you meet APCERT Operational Member requirements?

Yes

Operational Member

No

Liaison Partner

No

Strategic Partner

No

Are you a not-for-profit or government organisation with cyber security responsibilities?

Yes

Are you a commercial entity?

No

Corporate Partner

Yes

November 2017
Why do we need APCERT?

• Cyber threat landscape continues to evolve

• Range of threats is ever increasing – seeing two distinct trends
  1. Targeted: Increasingly sophisticated exploits are being developed and deployed against well-protected networks
  2. Broad-based: Criminals compromising networks using publicly known vulnerabilities that have known mitigations (eg WanaCry)

• Current challenges
  • Ransomware
  • Business Email Compromise / Social engineering
  • Targeting trusted third parties
  • DDoS

• The challenges are not national – they are regional and global
  • Theft of money, data (corporate & personal) and intellectual property
  • Extortion attacks such as denial of service and ransomware
  • Malware hosted on compromised websites
  • Spear phishing emails / Business email compromise – network access & fraud
APCERT Objective 1 – Security Cooperation

- 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
APCERT Objective 2 – Emergency Response

- 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 information security and emergency response capabilities across regional boundaries
APCERT Objective 3 – Security Awareness

- Organize and conduct an **annual AGM and APCERT Conference** to raise awareness on computer security incident responses and trends, exchange information on cyber security trends, discuss threats and challenges, and assist government & critical entities.
How does APCERT work?

CSIRT (Computer Security Incident Response Team)
- Independent from politics, industry, market...
- Do not focus on WHO and WHY, focus on WHAT and HOW from a technical coordination perspective

CSIRT Common Policy
- MY security depends on YOUR security
- Web of trust

Systematic Handling
- Timely manner
- Each team has appropriate domestic contacts to handle and respond to incidents (ISPs, critical infrastructure, government...)
- Mailing lists, Traffic Light Protocol, encrypted e-mail
- Reaching to disconnected areas using CSIRT network

POC arrangement between members
- One Point of Contact per economy
- Deal with serious and time critical computer security incidents
- Reachable 24 hours / 7 days via call
APCERT Working Groups

- **Malware Mitigation WG** (Convener: MyCERT)
  - To discuss security metrics in order to identify ways to improve on currently available security metrics, best practices on clean-up and data sharing methods

- **Information Sharing WG** (Convener: CNCERT/CC)
  - To identify information regarded as useful for APCERT members and/or available to share with other APCERT members

- **Membership WG** (Convener: KrCERT/CC)
  - To review the current membership criteria/classes

- **Policy, Procedures and Governance WG** (Convener: CERT Australia)
  - To promote the Vision and Mission of APCERT, To review the Operational Framework and other documents

- **Training WG** (Convener: TWNCERT)
  - To establish an overall education and training program to assist members to develop, operate, and improve their incident management capabilities.

- **TSUBAME WG** (Convener: JPCERT/CC)
  - To exchange analytical information of TSUBAME, the packet traffic monitoring system to observe suspicious scanning activities in the Asia Pacific and other regions.

- **Drill WG** (Convener: ThaiCERT)
  - To improve the efficiency and stability of the organization of the annual drill by maintaining a fixed organization that can learn from experiences each year.
# Capacity Building

**APCERT Online Training (bimonthly)**

<table>
<thead>
<tr>
<th>Date</th>
<th>Theme</th>
<th>Presenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 Feb 2017</td>
<td>Digital Forensics</td>
<td>Sri Lanka CERT</td>
</tr>
<tr>
<td>19 Apr</td>
<td>Mobile Vulnerability Check and Case Study</td>
<td>KrCERT/CC</td>
</tr>
<tr>
<td>1 Aug</td>
<td>Cyber Detection, Eradication and Forensic (Cyber D.E.F)</td>
<td>MyCERT</td>
</tr>
<tr>
<td>3 Oct</td>
<td>Cyber threat information sharing</td>
<td>CERT Australia</td>
</tr>
<tr>
<td>5 Dec</td>
<td>Introduction of DDoS Offensive and Defensive Exercise in Taiwan</td>
<td>TWNCERT</td>
</tr>
<tr>
<td>6 Feb 2018</td>
<td>Malware Information Sharing Platform (MISP) in a CERT</td>
<td>AusCERT</td>
</tr>
</tbody>
</table>
Recent and upcoming Activities

Updated APCERT Operational Framework
• New structure to include Partners

APCERT Information Classification Policy Update
• Updating APCERT Information Classification Policy in line with the ‘FIRST Standards Definitions and Usage Guidance — Version 1.0’

Capacity Building Survey
• Surveyed members in 2017 conducted to determine APCERT member strengths and gaps
• Capacity Development WG to be established: will use the skills and expertise of APCERT Members/Partners to share experiences and strengthen the APCERT community

Events presented as APCERT Representative:
• The OIC-CERT Annual General Meeting and Annual Conference
• APRICOT / FIRST TC / AP*
• APEC-TEL
Recent and upcoming Activities - APCERT Drill

Practice – APCERT Incident Handling Drill
- Conducted annually
- Participation from most of APCERT teams and some external organisations
- A simulation exercise of cyber attacks, includes communication checks based on given scenario.

Last Drill: 22 March, 2017
- Theme: “Emergence of a New DDoS Threat ”
- Participating Teams:
  - 23 CSIRTs from 18 economies
  - 4 CSIRTs from OIC-CERT
- Objective/Scenario:
  - Mitigate DDoS incidents triggered by a type of malware which has been widely observed in the Asia Pacific region

Next Drill: 7 March 2018
Recent and upcoming Activities - APCERT AGM & Conference

- 2017 APCERT AGM and Conference
  - Date: 12-15 November, 2017
  - Hosted by: CERT-In (India), Delhi
  - Theme: “Building Trust in the Digital Economy”

- 2018 APCERT AGM and Conference
  - Date: Q4 2018
  - Hosted by: CNCERT/CC (China), Shanghai
  - Theme: TBA
APCERT Annual Report

- Activity reports of APCERT member teams
  - Overview and activities of each team
  - Team reports and statistics on incidents and trends
  - Projects and Activities

- Annual Report 2016 is available online

- Annual Report 2017 will be available soon
Thank you!

APCERT General Contact: apcert-sec@apcert.org

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