ANNUAL REPORT 2012

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM

MEMBER OF

APCERT
Asia Pacific Computer Emergency Response Team

ID-CERT Annual Report 2012
Table of Content

1. About ID-CERT

1.1. Introduction

ID-CERT (Indonesia Computer Emergency Response Team) is an independent team which is from and for community. ID-CERT is the first CERT in Indonesia and founded by Budi Rahardjo, MSc., PhD. in 1998. ID-CERT together with JP-CERT (Japan), AusCERT (Australia) is one of the founders of the APCERT (Asia Pacific Computer Emergency Response Team) forum.

1.2. Establishment

In 1998 there was no CERT in Indonesia. Based on that Budi Rahardjo, MSc., PhD., an internet security expert, encouraged himself to establish ID-CERT. At the same time countries around Indonesia began to establish their own CERTs and this continued into Asia-Pacific forum which later became the APCERT.

ID-CERT wishes to remain standing as a non-governmental organization, independent, but received an allocation of government funding as a contribution to the CERT. ID-CERT is just being reactive (not active) in responding and handling a case of incoming or reported incident by complainers, either locally and internationally. ID-CERT does not have the authority to investigate a case thoroughly, but just become a liaison who can be trusted, especially by those who reported incident.

1.3. Workforce Power

During 2011 complaints received by ID-CERT were still handled by Budi Rahardjo, MSc., PhD. and Andika Triwidada. January 2011, Ahmad Alkazimy was recruited after being volunteer in research activity since March, 2007. Then, Rahmadian L. Arbianita joined the team since January 2012.

Volunteers :

1. Budi Rahardjo, MSc., PhD. ***(ID-CERT Chair)***
2. Andika Triwidada ***(ID-CERT Co-Chair)***
   Finger print: 5568 7C7D E898 4F33 A594 A996 DA4B C29F E22D FEE7
3. Maman Sutarman
4. Ikhlasul Amal
5. Rizky Ariestiyansyah
6. Other volunteers

Professional Staffs :

1. Ahmad Alkazimy (***ID-CERT Manager***)
   e-Mail: ahmad@cert.or.id
   Mobile: +62-838-74-9292-15
   Finger print: 39B2 87BA 3DD6 7832 D56F 0344 FCE4 3A7C FE38 CC96
2. Rahmadian L. Arbianita (***Incident Response Officer – HelpDesk***)
   e-Mail: rahmadian@cert.or.id
   Mobile: +62-811-22-77-03
   Finger print: 414A 1183 199E 8BA5 E0D1 C234 08BF 8BDE 1766 2CC7

1.4. Community Support

ID-CERT wishes that more respondents will be participated in the various studies conducted by ID-CERT, in order to make a better internet in Indonesia in the future. ID-CERT also wishes that the efforts in building all of this can have support in ID-CERT operations.

1.4.1. Constituent

ID-CERT Membership is open to all Indonesia Internet community who are concerned in the internet security, either from the ISP or non-ISP, such as government organizations (ministries, local governments, state enterprises, enterprises, etc.) as well as private citizens.

1.4.2. ***Respondent***

Now ID-CERT has 38 organization respondents participating in Internet Abuse Research. ID-CERT still welcome to new respondents who wish to join in the various researches/studies conducted by ID-CERT.

1.4.3. ***Affiliation***

ID-CERT defines that ID-CERT supporter or affiliate is the organization that have supported in ID-CERT research.

ID-CERT still welcome and invite Indonesia Internet community to support ID-CERT in a way of sponsorship, donations or through the mechanism of Membership Fees (to be determined later).

1.4.4. ***Volunteer***

From the start, ID-CERT are supported by many volunteers who work selflessly to contribute and concern for internet security in Indonesia. Generally, ID-CERT volunteers are individual one.

ID-CERT also welcome a wide opportunity for individuals who want to contribute to Indonesia internet security by being one of ID-CERT researchers or help desk officers.

2. Mission

ID-CERT missions are:

1. ID-CERT does not have operational authority to its constituency, either in Indonesia or abroad, but only to inform the various complaints of network incidents, and relies entirely on the cooperation with the parties involved in the incident related networks.
2. ID-CERT is built by the community and the results will be given back to the community.
3. ID-CERT helps to socialize the importance/awareness of internet security in Indonesia.
4. ID-CERT is undertaking various researches in internet security required by the internet community in Indonesia.
5. ID-CERT mission is to coordinate the incident handling involving local and international communities.

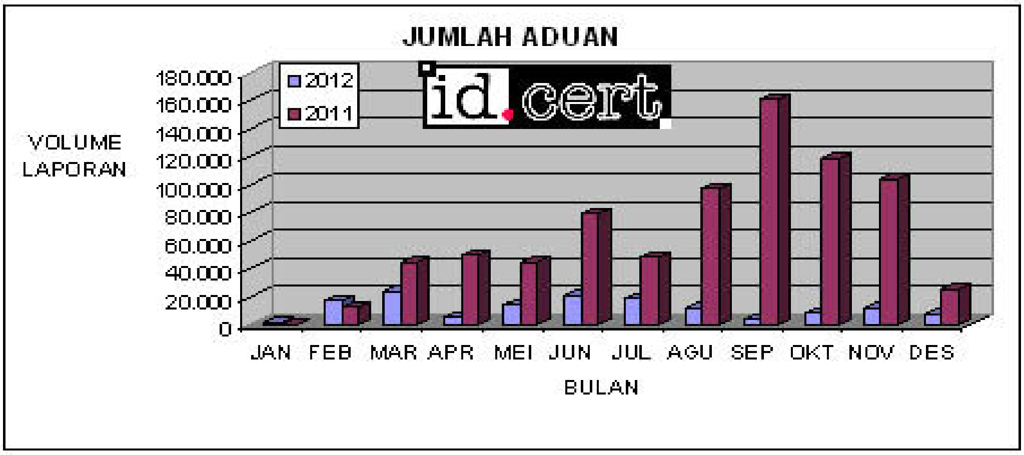
3. Activities

ID-CERT is a reactive CERT. From all complaints received by ID-CERT, Network Incident is the biggest amount reported. These reports/complaints which were once received by individuals - usually received by Budi Rahardjo, MSc., PhD., Andika Triwidada, and Ahmad Alkazimy - in the year 2012 has begun received on a particular email and handled by a professional staff of ID-CERT, which is then forwarded to the sites reported problems or to the related service provider. Additionally, other media used to describe the case and its development is the mailing list.

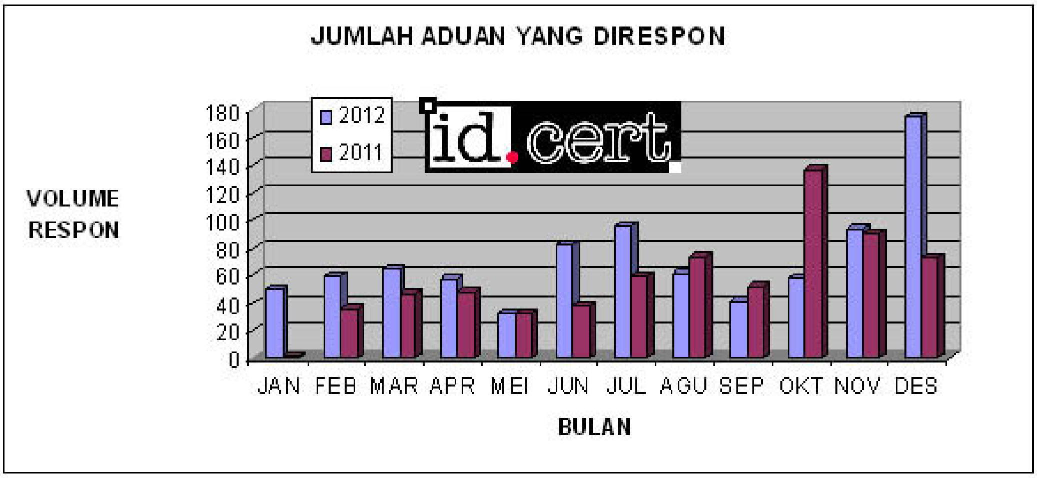
Now, ID-CERT has a HelpDesk that manages the received reports/complaints and the progress report completion. Currently, ID-CERT is run by professionals and supported by volunteers. The demand for the HelpDesk is related to service and handle the complaints of incident, as well as the statistical purposes to display cases handled, which is always presented at APCERT AGM.

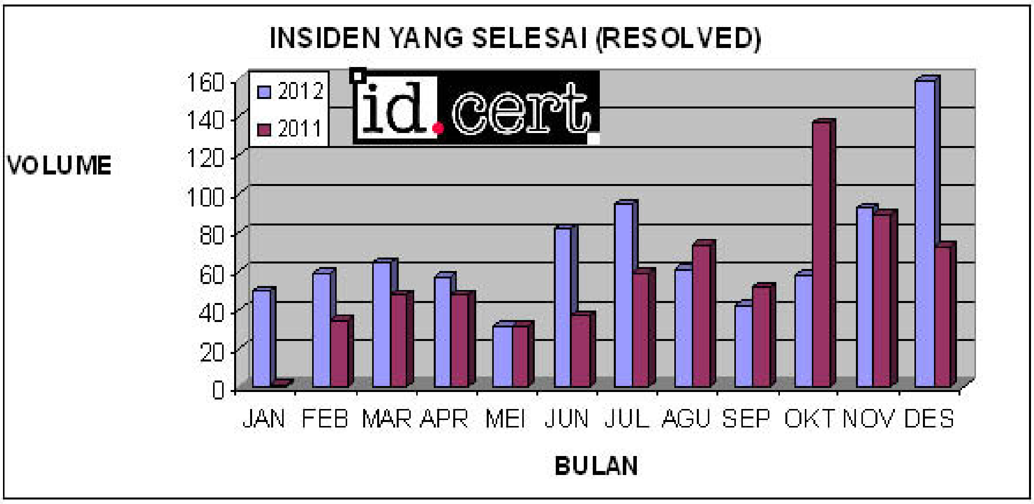
3.1. Incident Handling

At December 31, 2012 ID-CERT had received 141,616 incident complaints during the year 2012.



ID-CERT had proceed 868 incidents and 852 of them had successfully handled and solved.





ID-CERT has made Standard Operation Procedures (SOP) relating to the incident handling with priority: the complaints that come from local and the international complaints that request for assistance. While the complaint incidents in the sent as a copy/cc (already addressed directly to the ISP) ID-CERT will not process it further.

Effective as of November 1, 2012, ID-CERT has handled fully all incidents according the SOP, which was previously only focused on Phishing/Spoofing complaints and government agencies complaints.

In order to expedite the handling and incident documentation process of complaints, effective on November 1, 2012 ID-CERT had also successfully operate the documentation and e-mail ticket system using RTIR.

3.2. Incident Monitoring Report (IMR)

Incident Monitoring Report (IMR) is a joint monitoring activity that involve active constituents of ID-CERT by sending email copy of the incident complaint.

In the last 2 years, ID-CERT has conducted research related to the handling of incidents based on complaints or it's called Incident Monitoring Report (IMR) by involving ISPs, NAPs, Telecommunication Operators, and non-ISPs, such as government and corporate institutions. Starting with the Internet Abuse Research in 2010, now as of March 2012, the research has become one of the ID-CERT routine activities and become permanent that expected to be sustainable, so that Indonesia can have a primary data on Incident Monitoring Report occurred in Indonesia.

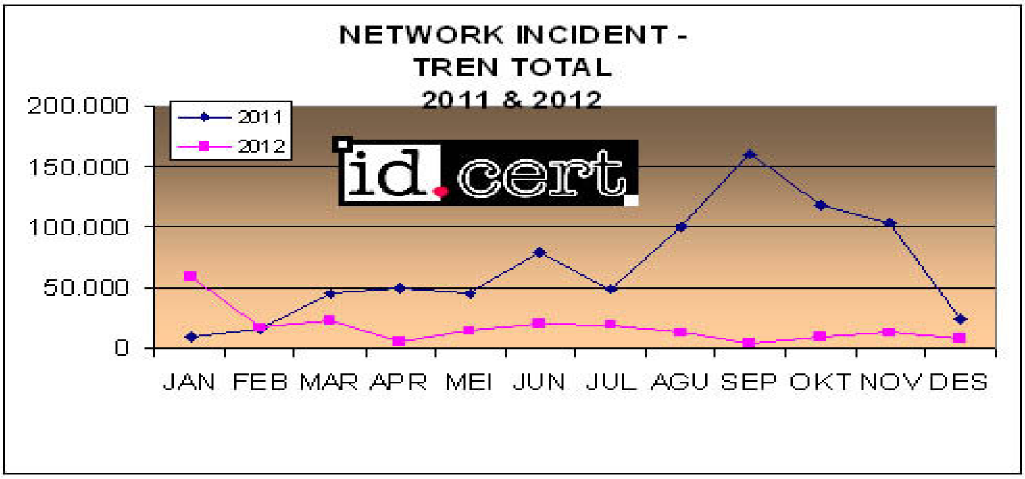
In contrast to the reports ID-CERT received above, reports received through IMR in the year 2012, when averaged over a number of reports of complaints are 290,297 reports per month. While the number of reports received during the year 2011 was reported as 1,057,333 or an average of 88,111 per month. And total number of reports received in 2012 is only 265,194.

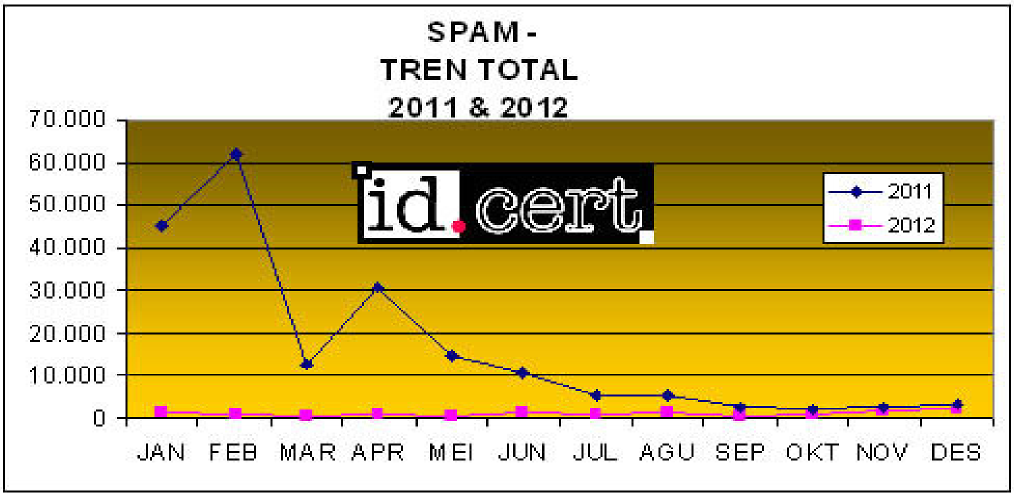
2012		
No.	Category	Rating (%)
1.	Network Incident	76,53
2.	**Malware**	8,63
3.	**Intellectual Property Rights/HaKI**	6,99
4.	**Spam**	4,78
5.	**Spam Complaint**	1,94
6.	**Spoofing/Phishing**	0,64
7.	**Response**	0,48

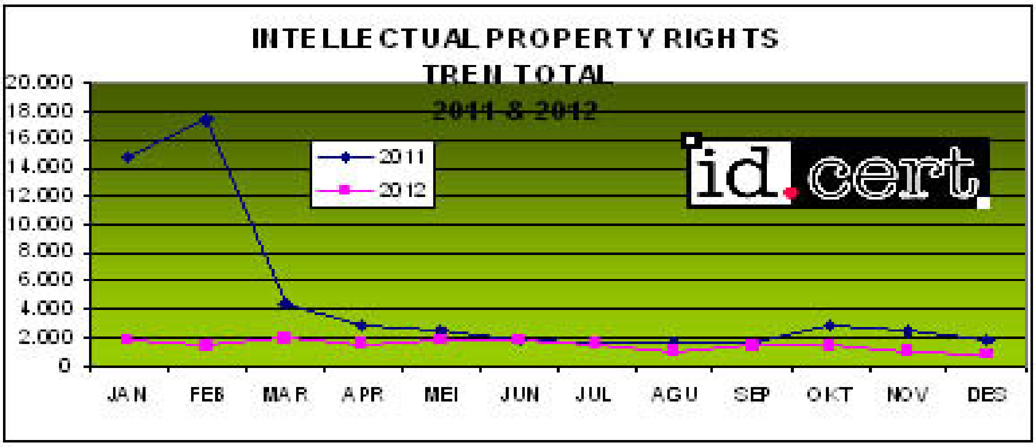
2011		
No.	Category	Rating (%)
1.	Network Incident	75,45
2.	Spam	17,40
3.	Intellectual Property Rights/HaKI	5,33
4.	Malware	1,62
5.	Spoofing/Phishing	0,11
6.	Response	0,07
7.	Spam Complaint	0,03

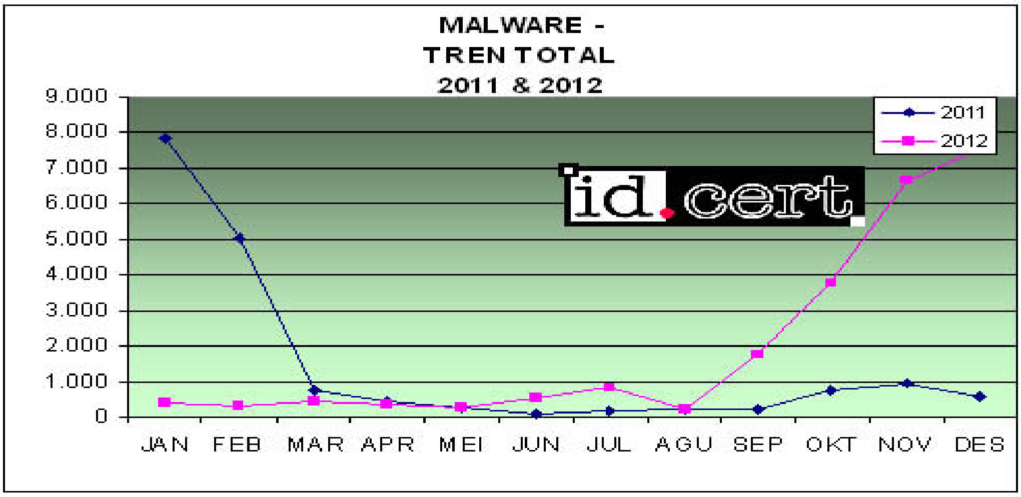
*Note: **in Bold:** position rating changing in 2012 compared to 2011*

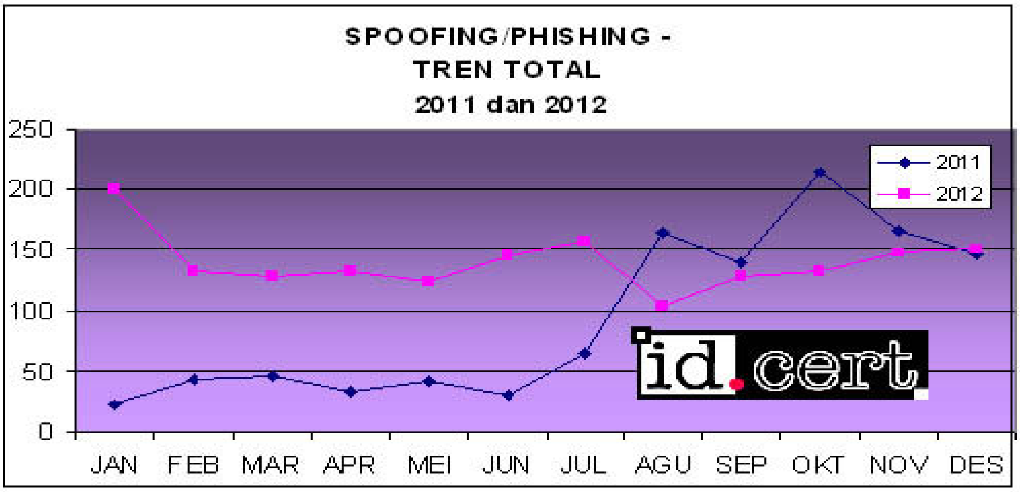
Here are comparison of trend graphs total in 2011 and 2012 for Network Incident, Spam, Intellectual Property Rights /IPR, Malware, Spoofing/Phishing, Response, and Spam Complaints:

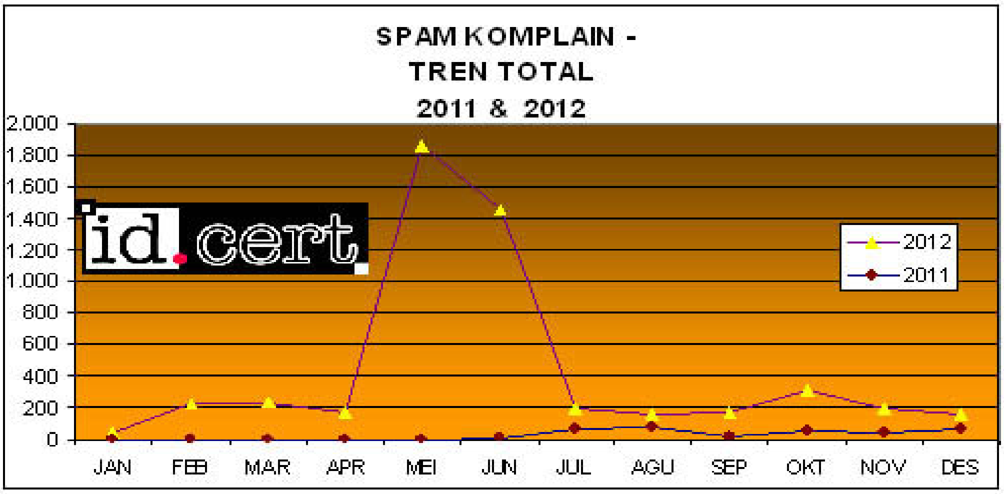





INTELLECTUAL PROPERTY RIGHTS
TREN TOTAL
2011 & 2012
2011
2012
id.cert
20.000
18.000
16.000
14.000
12.000
10.000
8.000
6.000
4.000
2.000
0
JAN
FEB
MAR
APR
MEI
JUN
JUL
AGU
SEP
OKT
NOV
DES


MALWARE -
TREN TOTAL
2011 & 2012
2011
2012
id.cert
9.000
8.000
7.000
6.000
5.000
4.000
3.000
2.000
1.000
0
JAN
FEB
MAR
APR
MEI
JUN
JUL
AGU
SEP
OKT
NOV
DES


SPOOFING/PHISHING -
TREN TOTAL
2011 dan 2012
2011
2012
id.cert
250
200
150
100
50
0
JAN
FEB
MAR
APR
MEI
JUN
JUL
AGU
SEP
OKT
NOV
DES



Complaints/Cases received by ID-CERT most of them are from other countries, after they found difficulty in contacting the administrator of the problematic website. ID-CERT is being a trusted party to report the case because ID-CERT has established good relationships with neighboring countries.

3.3. Security Warning/Advisory/Notice

Since November 2012, on the advice of a number of CERTs when occuring the Outbreak Malware Grumbot, the ID-CERT began issuing warnings in the Security Advisory form. This is the latest achievement of ID-CERT after all this time trying to find the right formula and type of Security Warning/Advisory/Notice which suitable for ID-CERT constituents.

By December 2012, ID-CERT has issued 5 (five) Security Warning/Advisory/Notice in Bahasa Indonesia.

3.4. Events

There are three major events attended by ID-CERT in 2012:

1. February 14, 2012 – APCERT Drill
2. February 29, 2012 – ID-CERT Gathering IV in Jakarta
3. March 25-28, 2012 – APCERT Annual General Meeting 2012 in Bali

4. Achievement

ID-CERT achievements in 2012 are:

1. ID-CERT has built a Standard Operation Procedures (SOP) and detail job desk to conduct staff development and personnel additions, at least for a response helpdesk.
2. ID-CERT has made the development of hardware and software associated with building a systemic mechanism email responder and updated ID-CERT website www.cert.or.id
3. ID-CERT has been conducting research required by the Internet community in Indonesia.
4. Since November 2012 ID-CERT officially began releasing Security Warning/Advisory/Notice on ID-CERT website and mailing list.
5. ID-CERT has published a research report on a regular basis: per bi-monthly, per semester, and annual report on the ID-CERT website.
6. ID-CERT got involved in the establishment of GovCSIRT from Roadmap to operational implementation.

5. Agenda

ID-CERT main concern is what actually expected by the public from ID-CERT.

1. ID-CERT plans to continue to conduct various researches and studies required by the Internet community in Indonesia. For that, the ID-CERT also plans to add personnel in the research/study and collaborate with leading universities in developing any needed research.
2. ID-CERT keeps periodically publish research reports per month, bi-monthly, per semester and annual/final report.
3. ID-CERT also wants the support of the constituents of public education in various sectors of internet security.