ID-CERT Activity Annual Report 2011
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 DR. Budi Rahardjo 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 DR. Budi Rahardjo, 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. 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 Dr. Budi Rahardjo and Andika Triwidada. Since January, 2011 Ahmad Alkazimy was recruited after being volunteer in research activity since March, 2007.

1.4. Constituency & Etc.

At the end of 2011, ID-CERT had successfully expanded its constituencies to ISP, NAP, Government bodies, ccTLD-ID Registry, Corporates, Professional Associations and individuals.

In addition, ID-CERT also had succeeded in formulating its mission together with the community and its constituents. The missions are:

1. ID-CERT's purpose is to coordinate the incidents handling involving community locally and internationally.
2. ID-CERT does not have operational authority to its constituency, it only informs a variety of complaints to network incidents, and depends entirely on the cooperation with all those involved in incidents related networks.
3. ID-CERT is built from community and the results will be given back to the community.
4. ID-CERT helps increasing the internet security awareness in Indonesia.
5. ID-CERT has research in internet security which is needed by the Indonesia internet community.

2. Activities and Operations

2.1. Activities

2.1.1. Incident Handling Reports

Abuse category consists of:

Spam	Spam complaints received from abroad to the network in Indonesia
Spam Complaint	Spam complaints received from domestic/local to the network in Indonesia and abroad
Response	The response provided by all parties on incoming reports
Network Incident	Activities carried out on other people's networks as well as all activities related to network abuse
Fraud	Report misuse of credit cards. This definition is based on reports police/law enforcement
Spoofing / Phishing	E-mail scams and websites to deceive users
Malware	A computer program created with malicious intent
IPR	Intellectual Property Rights

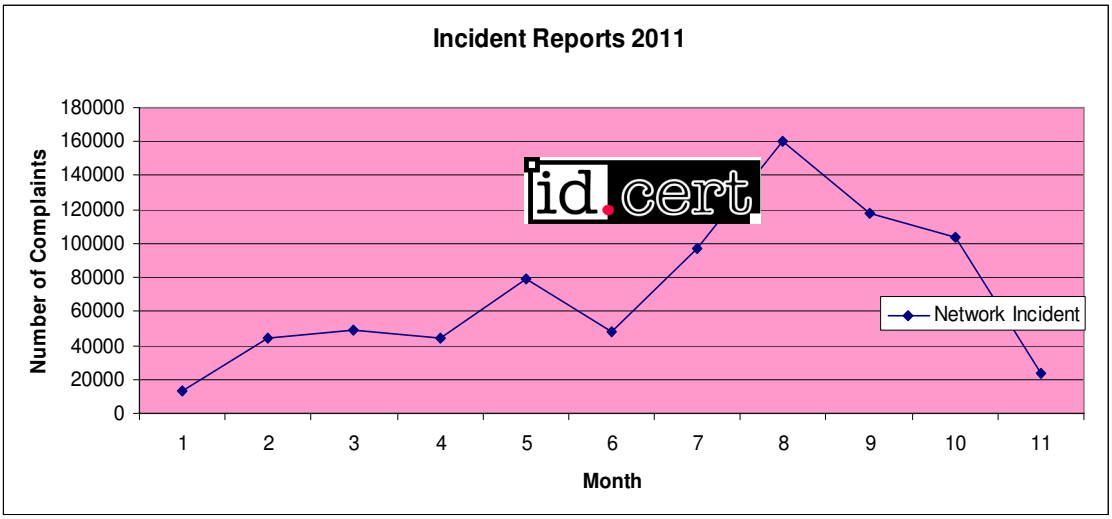

Figure 1: Incident Handling Reports 2011

Most of the complaints that ID-CERT received on 2011 from the communities were Network Incident.

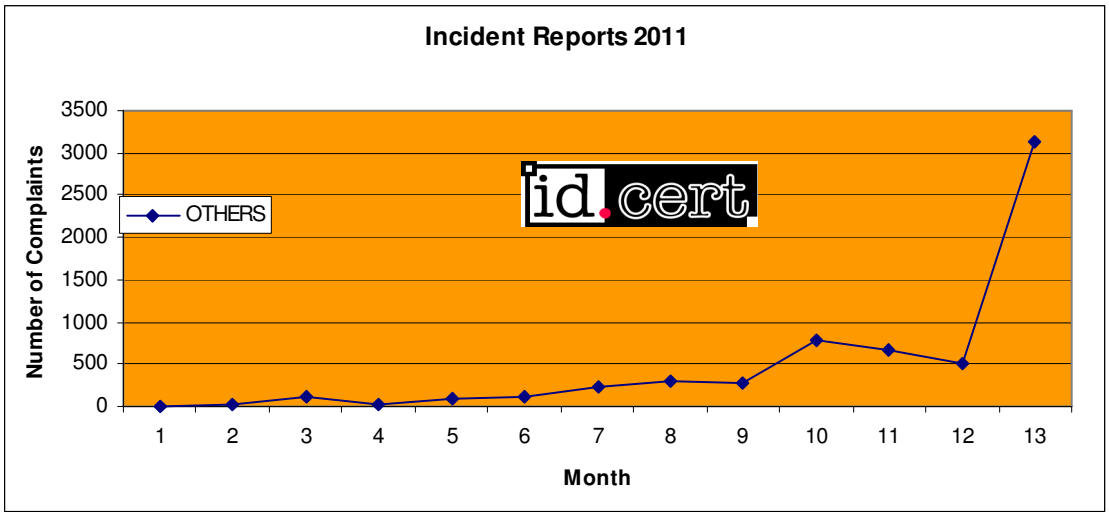

Figure 2: Incident Handling Reports 2011

Other complaints that ID-CERT received were: Malware, Spoofing/Phishing, Spam, Spam Complaints and Response.

2.1.2. Research on Indonesia Internet Abuse 2011

The research initiated several years ago in creating Internet Security statistics based on reports received by ID-CERT only.

In 2011 ID-CERT added more respondents to get more data besides the current one from ID-CERT. Totally 45 respondents had joined the Internet Abuse research by the end of 2011, including ID-CERT, PANDI (ccTLD-ID Registry), 3 Ministry Offices, 5 telecommunication operators, 7 NAPs, 25 ISPs, and 2 foreign respondents. The type of data ID-CERT got from the respondents were Summaries of Abuse reports received by each respondent or email copies of Abuse reports received by each respondent.

In contrast to reports received by the ID-CERT itself, the amount of average consolidated complaint received through Internet Abuse Research in 2011 amounted to 26,095 reports.

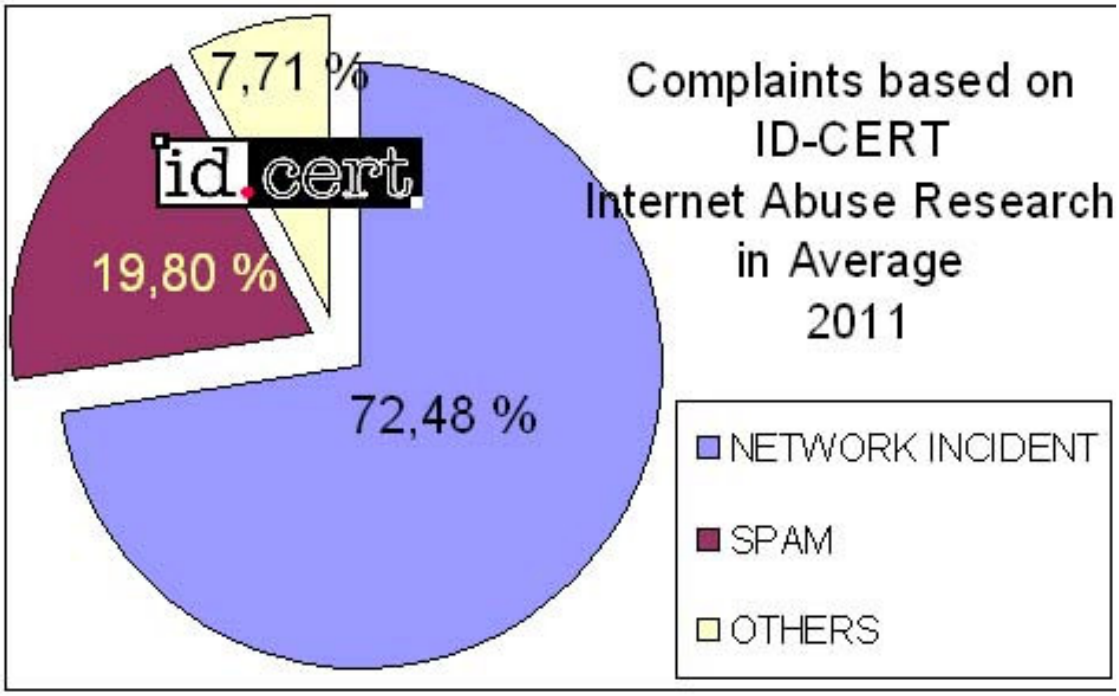

Figure 2: Research on Indonesia Internet Abuse Statistics 2011 (Monthly average, in %)

Figures shown above were the average abuse complaints ID-CERT received from the 43 local and 2 foreign respondents. The biggest level was the network incident, followed by the second large complaints were the spam.

2.2. Operations

E-mail abuse@cert.or.id was activated in January 1, 2011 to receive data from Research on Internet Abuse respondents.

E-mail cert@cert.or.id was also created to receive complaints.

ID-CERT plans to create some complaint e-mails which clasified based on most reports received.

3. Events

In February 28, 2011 ID-CERT had its third Public Gathering in Jakarta. A number of topics were discussed in the gathering, they are:

1. Current and future services
2. Abuse Research update
3. Funding
4. Formalizing ID-CERT Framework based on RFC2350.

In March 22-25, 2011, the APCERT AGM was held in Jeju, South Korea. ID-CERT could attend it after absent for several years. Thanks to APCERT and KrCERT for facilitating it.

4. Collaboration

4.1. Local

In July 2011 the first meeting between ID-CERT and APJII continued to have an MoU in November 2011.

ID-CERT also added its service by providing feed report to KAMINFO (Directorate of Information Security, Ministry of Communication and Information) regarding to government sites which got defacing/phishing.

ID-CERT was invited several times by KAMINFO in some events, such as Workshop of Handling Information Security Incident and Indonesia Internet Security Forum (IISF), and as a keynote speaker in CERT Regulation meeting.

4.2. International

ID-CERT got email feed from some foreign organizations for all IP address and domain names related to Indonesia. Some foreigner CSIRTs from Europe to Latin America (including GovCERT and Financial CERT) often make coordination with and asking help from ID-CERT.

5. Future Plan

ID-CERT has a number of plans related to future development of ID-CERT.

First thing to do, ID-CERT will employ several full-time staffs to increase incident handling capacity. A response help desk officer will be recruited soon. ID-CERT will also plan to send its staff for an internship to another CERT. It means that the employee of ID-CERT could have a complete picture of CERT services in general.

Second one, ID-CERT will deploy a system to manage and handle incidents better. ID-CERT will prepare the workflow and Standard Operation Procedures (SOP).

In addition, research activities, such as Abuse Research, a local product of ID-CERT for the needs of their constituents, will continue to work on. ID-CERT plans to maintain the data until the next few years.

ID-CERT will prepare several other researches and studies, required by Indonesia internet community. ID-CERT also plans to add personnel in the field of research and collaboration with leading universities in developing any necessary research.

ID-CERT will publish regular research reports per month, per bi-monthly, per semester, and annual report.

The last, the most ID-CERT's attention is: what exactly will be expected by society from ID-CERT.

6. Contact Information

Web : http://www.cert.or.id

E-mail : cert@cert.or.id (incident complaint)
abuse@cert.or.id (Internet Abuse Research)

Phone : +62 838 74 9292 15 (Mr. Ahmad Alkazimy)

PGP Keys :

Mr. Andika Triwidada
E-mail: andika@cert.or.id
Fingerprint=5568 7C7D E898 4F33 A594 A996 DA4B C29F E22D FEE7

Mr. Ahmad Alkazimy
E-mail: ahmad@cert.or.id
Fingerprint=39B2 87BA 3DD6 7832 D56F 0344 FCE4 3A7C FE38 CC96

7. Conclusion

After facing the hard times, ID-CERT attempted to rise again as a community-based CERT.

As for the future based on ID-CERT's views: in Indonesia, will appear more sectors CERT such as banking CERT, government CERT, education CERT, etc based on the need of their own community to coordinating to each other.

In the year 2011, though only a few abuse reports that come in, ID-CERT planned to continue enhancing the ability of ID-CERT personnel through training and plan for internship.

Another issue that ID-CERT found last year was the difficulty to contact the content provider/social networking providers such as Facebook, Twitter, Yahoo and Google. Finally, the issues had been resolved. Thanks to APCERT team.