APCERT Annual Report 2009

APCERT Secretariat
E-mail: apcert-sec@apcert.org URL: http://www.apcert.org

APCERT
Asia Pacific Computer Emergency Response Team

CONTENTS

Chair's Message 2009 3

I. About APCERT 5

1. Objectives and Scope of Activities 5
2. APCERT Members 7
3. Steering Committee (SC) 8
4. Working Groups (WG) 9
5. APCERT Website 10

II. APCERT Activity Report 2009 11

1. International Activities and Engagements 11
2. Approval of New General Members / Full Members 15
3. APCERT SC Meetings 15

III. Activity Reports from APCERT Members 16

Full Members 16

1. AusCERT Activity Report 16
2. BKIS Activity Report 24
3. BruCERT Activity Report 29
4. CERT-In Activity Report 34
5. CNCERT/CC Activity Report 44
6. HKCERT Activity Report 53
7. JPCERT/CC Activity Report 57
8. KrCERT/CC Activity Report 63
9. MyCERT Activity Report 70
10. PHCERT Activity Report 77
11. SingCERT Activity Report 81
12. SLCERT Activity Report 83
13. TWCERT/CC Activity Report 91
14. TWNCERT Activity Report 105
15. VNCERT Activity Report 110

General Members 116

16. BDCERT Activity Report 116

Chair's Message 2009

HKCERT was honoured to serve as the Chair of the APCERT in 2009. It is my pleasure to report to members on the work that the Steering Committee has accomplished in the past year.

The Conficker worm that hit the internet last year posed a major threat to the community. However, at the same time, it gave us opportunity to demonstrate how well CERT teams can collaborate to tackle incidents, in particular in the Asia-Pacific region. In March and April last year, we have seen a lot of communications within the APCERT teams – teams shared the samples of the worm; sent out list of infected machines captured on their sensors; discussed handling strategies; distributed the analysis results of the worm; and worked together to monitor the activities of the worm. All these activities have helped build up a closer working relationship among member teams. And this is exactly why we started the APCERT 7 years ago (as stated in the mission of the Operational Framework). There will definitely be more threats of this kind in the years to come. With such close collaboration among team members, I am sure any extraordinary issues will be well handled by our members with such collaborative effort.

The APCERT Drill is another occasion where our members can build up a better working relationship. This year, 16 teams from 14 economies participated in the drill, and many other teams participated as observers to learn from this exercise. The organizing committee will summarize the lessons learned to improve our response capabilities and the cross border co-ordination procedures. Participating team will find the exercise useful and the annual drill will be one major event that we would like to continue to organize in future.

I consider the working relationship a very important element in our day-to-day response work. The working relationship is not just among member teams in the region, but also groups and other organizations throughout the world. In the past years, we have established links with regional CERT team groups, internet infrastructure organizations, and security research groups. This has

brought to us a broader reach out to other partners with the same objective to improve the availability and accessibility of the Internet. I hope we can maintain and expand our connection with these groups in future.

We have contributed to the establishment of new CERT teams in the region, and tried to bring these teams to the APCERT community. We have accepted one new general member and one full member this year. There are several membership applications on the pipeline and the steering committee will review these applications in the upcoming meeting. We have formed a working group on Code of Conduct, trying to define the responsibilities and expected behavior of a member team. There may be some updates on the operational framework as a result. The working group will keep all members informed if there is any outcome from the group.

I would like to take this opportunity to thank the steering committee members, in particular the deputy chair and Secretariat for their contribution last year. I look forward to the continual support from our members to make the APCERT very successful organization in the years to come.

Roy Ko
Chair of APCERT
Centre Manager, HKCERT
March 2010

I. About APCERT

1. Objectives and Scope of Activities

APCERT *(Asia Pacific Computer Emergency Response Team)* is a coalition of the forum of CERTs *(Computer Emergency Response Teams)* and CSIRTs *(Computer Security Incident Response Teams)*. The organization was established on February 2003 to encourage and support the activities of CERTs/CSIRTs in the Asia Pacific region.

APCERT will maintain a trusted contact network of computer security experts in the Asia-pacific region to improve the regions' awareness and competency in relation to computer security incidents through:

1. enhancing Asia-Pacific regional and international cooperation on information security;
2. jointly developing measures to deal with large-scale or regional network security incidents;
3. facilitating information sharing and technology exchange, including information security, computer virus and malicious code, among its members;
4. promoting collaborative research and development on subjects of interest to its members;
5. assisting other CERTs and CSIRTs in the region to conduct efficient and effective computer emergency response;
6. providing inputs and/or recommendations to help address legal issues related to information security and emergency response across regional boundaries.

The formation of CERTs/CSIRTs at the organizational, national and regional levels is essential to the effective and efficient response to computer security incidents, widespread security vulnerabilities and incident coordination throughout the region. One important role of CERTs/CSIRTs is education and training to raise awareness and encourage best practice. APCERT coordinates activities with other regional and global organizations, such as the Forum of incident Response and Security Teams (FIRST) <www.first.org>, and TF-CSIRT, a task force that promotes collaboration between CSIRTs at the European level <www.terena.nl/tech/task-forces/tf-csirt/>.

The geographical boundary of APCERT activities are the same as that of APNIC. The region covers the entire Asia-Pacific, comprising of 56 economies. The list of those economies is available at:

http://www.apnic.net/about-APNIC/organization/apnics-region

At present, APCERT Chair is HKCERT (Hong Kong Computer Emergency Response Team Coordination Centre). Deputy Chair is SingCERT (Singapore Computer Emergency Response Team). JPCERT/CC (Japan Computer Emergency Response Team/Coordination Center) serves as secretariat.

URL: http://www.apcert.org
Email: apcert-sec@apcert.org.

2. APCERT Members

APCERT was formed in 2003 by 15 teams from 12 economies across the Asia-Pacific region, and has increased its membership since then. In 2009, ID-SIRTII (Indonesia Security Incident Response Team of Internet Infrastructure) has been approved as General Member of APCERT. Also, SLCERT (Sri Lanka Computer Emergency Response Team) has upgraded its membership to Full Member of APCERT.

APCERT now consists of 23 teams from 16 economies across the AP region, of which 17 teams are full members and 6 teams are general members.

Full Members

Team	Official Team Name	Economy
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
CERT-In	Indian Computer Emergency Response Team	India
CNCERT/CC	National Computer network Emergency Response technical Team / Coordination Center of China	People's Republic of China
HKCERT	Hong Kong Computer Emergency Response Team Coordination Centre	Hong Kong, China
ID-CERT	Indonesia Computer Emergency Response Team	Indonesia
JPCERT/CC	Japan Computer Emergency Response Team / Coordination Center	Japan
KrCERT/CC	Korea Internet Security Center	Korea
MyCERT	Malaysian Computer Emergency Response Team	Malaysia
PHCERT	Philippine Computer Emergency Response Team	Philippine
SingCERT	Singapore Computer Emergency Response Team	Singapore
SLCERT	Sri Lanka Computer Emergency Response Team	Sri Lanka
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
VNCERT	Vietnam Computer Emergency Response Team	Vietnam

General Members

Team	Official Team Name	Economy
BDCERT	Bangladesh Computer Emergency Response Team	Bangladesh
BP DSIRT	BP Digital Security Incident Response Team	Singapore
BruCERT	Brunei Computer Emergency Response Team	Negara Brunei Darussalam
GCSIRT	Government Computer Security and Incident Response Team	Philippine
ID-SIRTII	Indonesia Security Incident Response Team of Internet Infrastructure	Indonesia
NUSCERT	National University of Singapore Computer Emergency Response Team	Singapore

3. Steering Committee (SC)

Since the last APCERT AGM held in March 2009, Chinese Taipei, the following members served as APCERT Steering Committee (SC).

- HKCERT (Chair)
- SingCERT (Deputy Chair)
- AusCERT
- KrCERT/CC
- JPCERT/CC (Secretariat)
- MyCERT
- ThaiCERT

4. Working Groups (WG)

5 Working Groups are formed within APCERT. In 2009, TSUBAME WG and Code of Conduct WG were newly formed.

1. Accreditation Rule WG

Objective: To develop an accreditation scheme for APCERT members
Members: JPCERT/CC (Chair), AusCERT, HKCERT, KrCERT/CC and MyCERT

2. Training & Communication WG

Objective: To discuss a training mechanism within APCERT (i.e. information exchange, CERT/CSIRT training)
Members: TWCERT/CC (Chair), AusCERT, KrCERT/CC, MyCERT and SingCERT

3. Finance WG

Objective: To discuss membership fee in the short run and develop a concrete scheme in the long run
Members: JPCERT/CC (Chair), AusCERT, HKCERT, KrCERT/CC, TWCERT/CC and TWNCERT

4. TSUBAME WG

Objectives:

- Establish a common platform for Internet threat monitoring, information sharing & analyses in Asia-Pacific region
- Promote collaboration among CSIRT in Asia-Pacific region by using the common platform
- Enhance capability of global threat analyses by incorporating 3D Visualization features to the common platform

Members: JPCERT/CC (secretariat) and TSUBAME project members

5. Code of Conduct WG

Objective: To review the existing practices and to define the responsibilities of APCERT members in areas of APCERT as a community
Members: Steering Committee, BKIS and SLCERT

5. APCERT Website

JPCERT/CC manages and updates the APCERT website <www.apcert.org>. On a temporary basis, AusCERT hosts the Point of Contact (POC) information for APCERT POC teams. Access is by password only for APCERT teams.

II. APCERT Activity Report 2009

1. International Activities and Engagements

APCERT has been active in representing and promoting APCERT in various international events. During March 2009 to February 2010, APCERT members have hosted, participated and/or contributed in the following events:

APCERT AGM & Conference 2009
3-5 March 2009, Chinese Taipei, hosted by TWCERT/CC
http://apcert2009.cert.org.tw/apcert2009/

APCERT 2009 was the 8th APCERT annual event, providing a valuable platform for APCERT members and CERTs/CSIRTs in the Asia-Pacific region, as well as closely related organizations and regional information security professionals, to come together and share trends, experiences and challenges in the Internet security field – especially on latest incidents and new initiatives to combat cyber attacks. It was a valuable opportunity to learn, share information and network with global and regional experts, and to raise the capacity of addressing large-scale and cross-border security incidents through a trusted relationship.

APEC TEL 39
13-18 April 2009, Singapore
https://app.apectel39.ida.gov.sg/home.aspx

- APCERT Chair (HKCERT) shared a presentation on APCERT collaborative responses on Conficker worm.
- MyCERT shared a presentation on the APCERT Cyber Exercise Drill 2008
- JPCERT/CC shared a presentation on the TSUBAME Internet traffic monitoring data visualization project
- APCERT SC held a meeting in conjunction with APEC TEL 39

21st Annual FIRST Conference Kyoto

28 June – 3 July 2008, Tokyo, Japan
http://conference.first.org/2009/

JPCERT/CC served as the local host of 21st Annual FIRST Conference Kyoto, focusing on the theme Aftermath: Crafts and lessons of incident recovery.
APCERT SC and members held a meeting in conjunction with FIRST 2009.

Indonesia Cyber Security Seminar
14 July 2009, Jakarta, Indonesia

ID-SIRTII and Ministry of Communication and Information Technology of Indonesia hosted a Cyber Security Day in Indonesia with the theme "Secure Your Information."
APCERT secretariat shared a presentation on APCERT activities.

ASEAN CERT Incident Drill (ACID) 2009
23 July 2009

The ASEAN CERT Incident Drill (ACID) 2009 was held on 23 July 2009, successfully coordinated by SingCERT. It was the fourth ACID with 14 participating teams from ASEAN CERTs and its dialogue partners this year, with the theme on Botnet.

AP* Retreat Meeting
23 August 2009, Beijing, China
http://www.apstar.org/apstar_agenda.php?p_content_category_id=2&p_meeting_id=29

APCERT Chair (HKCERT) shared a presentation on APCERT activity updates.
AP* Retreat Meeting gathers Internet-related organizations from the Asia Pacific region, to share their respective activities and to discuss issues that need to be considered as Asia-Pacific community, as well as to establish a trust relationship among the organizations. The meeting is held every once or twice a year.

Cyber Security Week 2009
25-28 August 2009, Colombo, Sri Lanka

SLCERT and ICTA (Information and Communication Technology Agency of Sri Lanka) hosted the second Cyber Security Week in Sri Lanka.
APCERT secretariat shared a presentation on APCERT activities.

Lao Information Security Seminar
14 September 2009, Vientiane, Laos

The Lao government hosted an Information Security Seminar to raise awareness of information security in Laos, and APCERT secretariat shared a presentation on APCERT activities.

APEC TEL 40
24-30 September 2009, Cancun, Mexico
http://apectel40.cft.gob.mx/

APCERT secretariat shared a presentation on APCERT activities as well as education/awareness efforts and outreach programs by APCERT members.

AVAR2009
4-6 November 2009, Kyoto, Japan
https://www.aavar.org/avar2009/sponsors.html.en

APCERT contributed as Supporting Partner of AVAR 2009 – 12th Association of anti-Virus Asia Researchers International Conference, the leading anti malware conference in the Asia-Pacific region.

December 2009 FIRST Technical Colloquium
1-2 December 2009
http://www.first.org/events/colloquia/dec2009/

CyberSecurity Malaysia and Team Cymru co-hosted the FIRST Technical Colloquium with a one-day plenary session and one-day hands-on session.

APCERT Drill 2010
28 January 2010

http://www.apcert.org/documents/pdf/Drill2010_PressRelease.pdf

APCERT Drill 2010, the 6th APCERT Cyber Exercise Drill, was successfully held with participation from 16 teams of 14 economies (Australia, Brunei, China, Chinese Taipei, Hong Kong China, India, Indonesia, Japan, Korea, Malaysia, Singapore, Sri Lanka, Thailand and Vietnam). The theme of the drill was "Fighting Cyber Crimes with Financial Incentives" and was coordinated by HKCERT, CNCERT/CC, MyCERT with scenarios designers of BKIS and SLCERT.

2nd PacCERT Working Group Meeting
11-12 February 2010, Suva, Fiji Islands
http://www.itu.int/ITU-D/asp/CMS/Events/2009/PACCERT/index.asp

The International Telecommunication Union (ITU) with support from the Department of Broadband, Communications and the Digital Economy (DBCDE), Australian Government, commissioned AusCERT to undertake a readiness assessment for establishing a Pacific regional CERT (PacCERT).
APCERT secretariat shared a presentation on APCERT activities in the 2nd PacCERT Working Group Meeting.

AP* Retreat meeting
28 February 2010, Kuala Lumpur, Malaysia
http://www.apstar.org/apstar_agenda.php?p_content_category_id=2&p_meeting_id=30

MyCERT shared a presentation on APCERT activity updates.
AP* Retreat Meeting gathers Internet-related organizations from the Asia Pacific region, to share their respective activities and to discuss issues that need to be considered as Asia-Pacific community, as well as to establish a trust relationship among the organizations. The meeting is held every once or twice a year.

Other International Activities and Engagements:

- **APEC TEL SPSG (Security and Prosperity Steering Group)**
  Mr. Jinhyun Cho of KrCERT/CC serves as Covenor of APEC TEL SPSG

- **DotAsia**
  APCERT serves as co-sponsor member of DotAsia

- **FIRST (Forum of Incident Response and Security Teams)**
  Ms. Yurie Ito of JPCERT/CC serves as Steering Committee and Board of Director of FIRST

2. Approval of New General Members / Full Members

Since the last APCERT AGM held in March 2009, Chinese Taipei, the following teams newly joined APCERT General Member / Full Member.

- SLCERT (Sri Lanka) was approved as Full Member as of 10 March 2009.
- ID-SIRTII (Indonesia) was approved as General Member as of 18 June 2009.

3. APCERT SC Meetings

Since the last APCERT AGM held in March 2009, Chinese Taipei, SC members held 2 meetings and 4 teleconferences to discuss on APCERT operations and activities.

III. Activity Reports from APCERT Members

Full Members

1. AusCERT Activity Report

Australian Computer Emergency Response Team - Australia

The following information contains information about AusCERT's activities during 2009.

1. ABOUT AusCERT

1.1 Introduction

Until 2010, AusCERT was the national CERT of Australia and operated in this role on a self-funded basis for many years. This role is now taken over by the Australian government-funded CERT Australia. AusCERT will provide services to CERT Australia, under contract.

As the national CERT, AusCERT served Australia's national interest by improving Internet security for Australian Internet users.

AusCERT does this by:

- collecting, analysing and providing advice about computer network threats and vulnerabilities;
- helping to mitigate Internet attacks directed at Australian Internet users and networks; and
- providing education and advice about issues affecting Internet security in Australia and globally.

1.2 Establishment

AusCERT was officially established on 8 March 1993 through the collaboration of three Brisbane based universities, including the University of Queensland. Over time, as the Internet grew and government, business and ordinary users began to use the Internet for daily communications and

business, AusCERT's focus changed from being university centric to include the interests of all sectors.

AusCERT is an independent, non-government, self-funded not-for-profit team of information and technical security professionals based at the University of Queensland. The University of Queensland is one of Australia's premier learning and research institutions.

1.3 Staffing

AusCERT employs 17 staff.

Constituency

During 2009, AusCERT's constituents were Australian Internet users in the public and private sector, home and business.

AusCERT works closely with Australian government agencies, industry and technology vendors and provides computer security and incident handling advice to a range of subscribers throughout Australia, New Zealand and the Asia-Pacific region. All Australian universities and the majority of New Zealand universities are members of AusCERT and there is a strong relationship with the Council of Australian University Directors of Information Technology (CAUDIT).

2. ACTIVITIES AND OPERATIONS

During 2009, AusCERT:

- provided incident response to help organisations mitigate Internet based attacks against their networks;
- mitigated online attacks that have compromised personal identity information (PII) by notifying the public and private sector organisations whose customers or clients have been affected;
- published security bulletins,[1] (including security bulletins about specific cyber threats affecting Australian networks and Internet users);

[1] See AusCERT security bulletins: https://www.auscert.org.au/1. AusCERT restricts public access to a small selection of security bulletins and papers in order to retain member value.

- published papers, policy submissions to government (relating to ICT and Internet security);[2]
- provided public outreach, education and awareness raising about Internet security issues by hosting workshops and through the media;
- provided information and expertise to law enforcement about specific cyber attacks affecting or emanating from Australian networks;
- participated in government, CERT and industry multi-lateral meetings including cyber security exercises with a range of global partners;
- communicated, cooperated and built relationships with industry, domain name registries, telecommunication providers and national CERT counterparts overseas.

2.1. Incident Handling

A large part of AusCERT's core business involves analysis of online cyber attacks. While these are not the only incidents handled by AusCERT, they represent a common form of cyber attack and show clear upward trends associated with these set of criminally-motivated activities.

Figure 1 shows the number of malware and phishing sites handled by AusCERT in 2009.

Each incident represents a single unique URL or domain name that is hosted by one or more compromised computers for the purpose of stealing sensitive information and access credentials from other computers. Multiple computer compromises can be associated with each attack, which is the set of compromised computers needed to launch the attack and collect the stolen data. The number of IP addresses involved in a single attack is variable but can range from 1 to around 5,000.

This graph does not include the number of computer infections (compromised hosts) that occur due to each malware attack of which there is generally many hundreds or thousands.

[2] See AusCERT publications http://www.auscert.org.au/1920

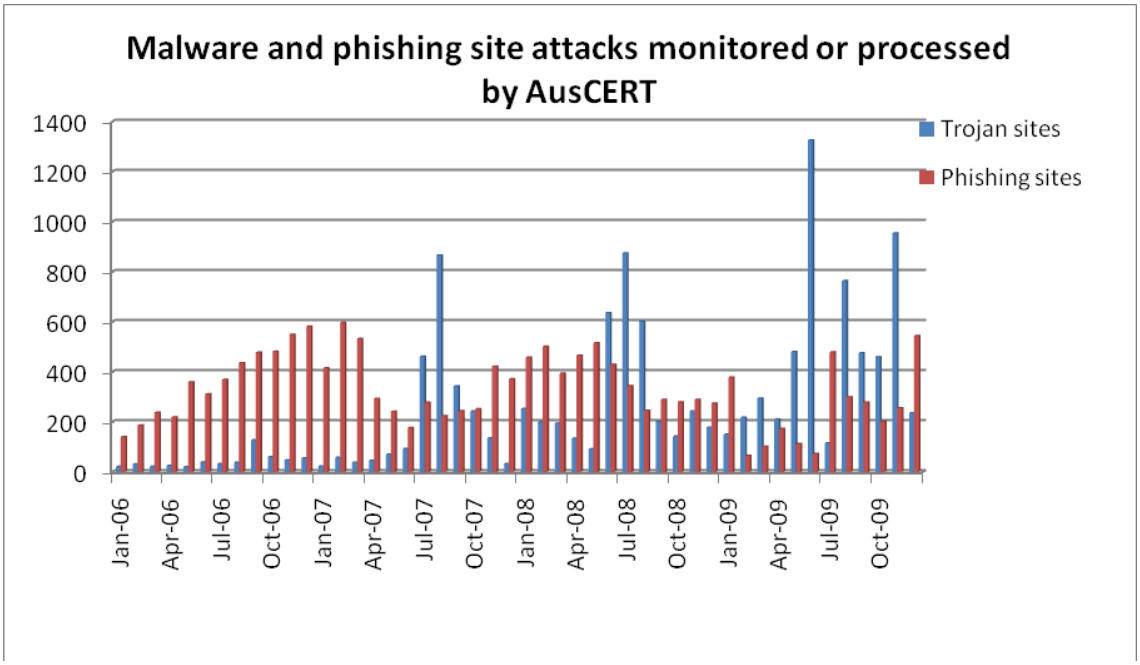
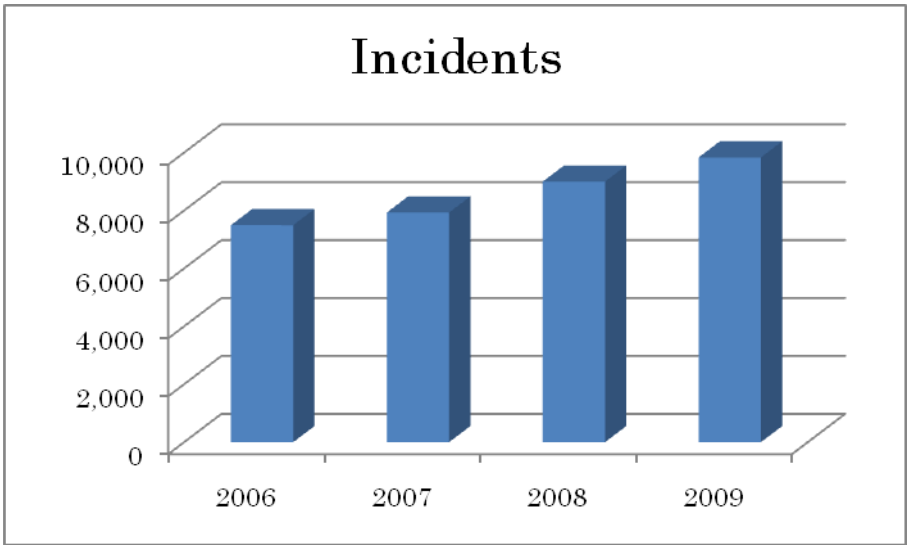


Figure 1

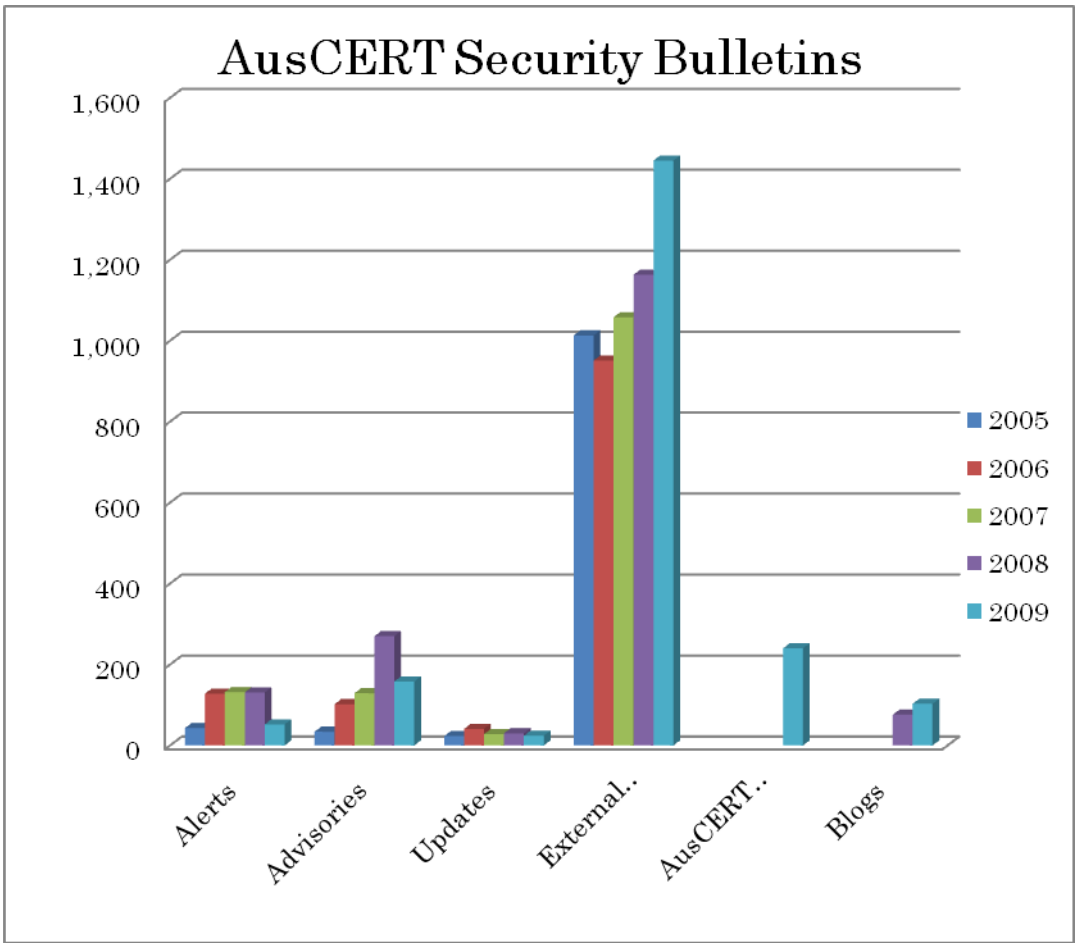
The figures above are representative of specific types of incidents handled by AusCERT. Total incidents handled are much greater.



2.2. Security bulletins and blogs

AusCERT publishes security bulletins as part of its services. In 2009, AusCERT changed its security bulletin format from one which included AusCERT alerts, advisories and updates to a simpler approach comprising only AusCERT Security Bulletins (ASB) and External Security Bulletins (ESB).

During 2009, AusCERT published 1,445 external security bulletins (ESB), and 577 AusCERT bulletins in the old and new formats. 103 blogs were published.



2.3. Network monitoring

AusCERT is collaborating with a number of partners operating monitoring projects, by hosting sensors.

2.4. Stay Smart Online Alert Service

In 2009 AusCERT continued to provide a service under contract from the Australian government, which is part of the government's broader Stay Smart Online initiative.[3] The Stay Smart Online Alert Service is a free service aimed at home users and SMEs with little or no technical knowledge. The service provides access to email, web and RSS feeds and includes a monthly

[3] www.staysmartonline.gov.au

newsletter and fact sheets.[4] AusCERT published 62 alerts and 27 advisories during 2009.

2.5. AusCERT Certificate Services (AusCERT-CS)

The AusCERT Certificate Service, which utilises Comodo certificate services, provides Australia's education and research community with SSL server certificates that are widely recognised by popular web browsers, mobile devices and other user applications.

Client certificates will be provided that can be used, among other things, to secure email communication and for TLS (Transport Layer Security) client authentication to identify persons accessing web sites. Code signing certificates will also be available. These are used to authenticate and sign software code for distribution over the Internet.

More information about the AusCERT Certificate Services is available from: http://cs.auscert.org.au

3. EVENTS ORGANISED / CO-ORGANISED

3.1 Training

AusCERT continues to provide CSIRT training upon request, including providing (Training of Network Security Incident Teams Staff) TRANSIT training in South Korea and FIRST TC training in Malaysia.

3.2 Conferences

AusCERT held its annual Asia-Pacific Information Security Conference at the Gold Coast Australia in May 2009 with over 1,000 delegates.[5] Coinciding with the annual AusCERT conference, AusCERT also hosts other networking and information sharing events. For example, AusCERT hosts an invitation only online crime symposium for key stakeholders and organisations that are most likely to be affected by this crime or are in a position to assist deal with the crimes.

[4] www.ssoalertservice.net.au

[5] conference.auscert.org.au/conf2009/

During 2009, AusCERT participated in a number of international conferences and events, including:

- APCERT2009, Chinese Taipei
- FIRST conference and technical colloquium
- ITU Cybersecurity Forum for Asia Pacific

4. ACHIEVEMENTS

4.1 Presentations and awareness raising

AusCERT has given presentations at several conferences throughout 2009. These include presentations at ITU Cybersecurity Forum in Hyderabad India, APEC-Tel, and the Underground Economy conference in France. In Australia, AusCERT briefed the Australian House of Representative's cybercrime enquiry and engaged with local industry groups in Australia including the Australian Computer Society and Australian secondary schools.

For the most part, these presentations have sought to give various communities knowledge of the cyber threat environment and allow them to consider whether their own preparations or strategic plans – be they at organisational, national or at international level are adequate to meet the needs of the current threat environment and future anticipated threats.

4.2 Publications

During 2009, AusCERT made a number of submissions to the Australian government, including into the area of cybercrime.[6]

During 2009, AusCERT prepared a scoping study to consider the feasibility of developing a regional CERT capability for the Pacific Island Nations, commissioned by the ITU. Details of this report are available on the ITU web site.[7] AusCERT continues to work with the ITU and stakeholders in the Pacific Island nations to progress this further.

[6] http://www.auscert.org.au/render.html?it=12024

[7] http://www.itu.int/ITU-D/asp/CMS/Docs/Interrim_PacificCERT_Report.pdf

5. INTERNATIONAL COLLABORATION

AusCERT continues to be actively involved with APCERT, serving on the Steering Committee again during 2009. AusCERT also manages the APCERT mailing lists and restricted web access to the APCERT Point of Contacts.

AusCERT also works closely with the UK Payments Administration (previously APACS), FIRST, Digital Phishnet, Anti Phishing Working Group, IMPACT, the ITU and European government CERTs and many open and closed information security groups.

2. BKIS Activity Report

Bach Khoa Internetwork Security Center - Vietnam

1. About Bkis - Vietnam

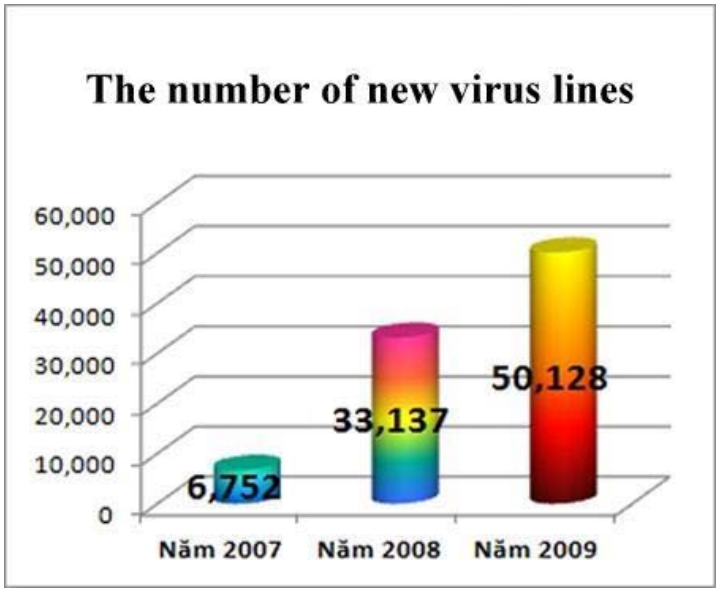
Bkis is a Vietnam's leading organization in researching, deploying network security software and solution. Bkis established on December 28th, 2001, and became full member of APCERT in 2003.

Head Office: 5th Floor, Hitech Building, Hanoi Unviversity of Technology, 1A Dai Co Viet, Hanoi, Vietnam

2. Activities & Operations

2.1. Security Statistics

Computer virus is the most headachy internet security issue in the past year. New lines of virus have been emerging in increasing number and complicated manner. There have been up to 50,128 new lines of viruses emerging in the past year, 1.5 times higher than 2008 and 7 times higher than 2007. These viruses have infected more than 64.7 million computers. The most infectious virus is W32.SalityVF.PE, which has infected more than 483,000 computers.



2.2. Top 15 viruses in Vietnam 2009

No	Virus name
1	W32.SalityVF.PE
2	W32.SalityVG.PE
3	W32.VetorI.PE
4	W32.TedrooG.Worm
5	W32.VodkaXAAN.Worm
6	W32.SecretKE1.Worm
7	W32.Wins.Trojan
8	W32.SvchostJJM.Trojan
9	X97M.XFSic
10	W32.VetorX5QWER.PE
11	W32.DownloadBZ.Worm
12	W32.ShopperHT.Adware
13	W32.KamsoftAD.Worm
14	W32.CimusPR.Worm
15	W32.GameDrop.Worm

2.3. Training Courses

Network Security Training Courses:

June 2009: For Engineers of Ministry of Public Security

June 2009: For Network Adminisrtators from companies (Banks, Securities...)

Security Awareness Training Courses:

July and September 2009 : 6 classes for BaoViet Finance – Insurance Group

2.4. Security Advisories

In the end of 2008 and 2009, we have discorvered and publised 21 advisories of the software vulnerabilities.

For reference, here is the list of advisories:

No	Advisory	Link
1.	Google Chrome “Save As” Function Buffer Overflow	http://security.bkis.vn/?p=119
2.	Microsoft Windows Media Encoder	http://security.bkis.vn/?p=176

	ActiveX Control Buffer Overflow	
3.	Critical Vulnerability in Hosting Controller allowing hackers to take control of server	http://security.bkis.vn/?p=239
4.	Vulnerability in WireShark 1.0.4 for DoS Attack	http://security.bkis.vn/?p=271
5.	Critical BoF vulnerability found in ffdshow affecting all internet browsers	http://security.bkis.vn/?p=277
6.	Multi security vulnerabilities in mvnForum 1.2 GA	http://security.bkis.vn/?p=286
7.	Google Wap Proxy Vulnerability can be exploited by Hackers to attack Internet Users	http://security.bkis.vn/?p=310
8.	Redirection Vulnerability in Yahoo! Advertising Service	http://security.bkis.vn/?p=324
9.	Vulnerability in Face Recognition Authentication Mechanism of Lenovo-Asus-Toshiba Laptops	http://security.bkis.vn/?p=292
10.	FeedDemon Buffer Overflow Vulnerability	http://security.bkis.vn/?p=329
11.	Multiple Vulnerabilities found in Rapidleech	http://security.bkis.vn/?p=345
12.	GOM Encoder Heap-based Buffer Overflow	http://security.bkis.vn/?p=352
13.	PowerCHM Stack-based Buffer Overflow	http://security.bkis.vn/?p=365
14.	GOM Player Subtitle Buffer Overflow Vulnerability	http://security.bkis.vn/?p=501
15.	010 Editor Multiple Buffer Overflow Vulnerabilities	http://security.bkis.vn/?p=580
16.	Microchip MPLAB IDE Buffer Overflow Vulnerability	http://security.bkis.vn/?p=654
17.	XSS vulnerability in PRTG Traffic Grapher	http://security.bkis.vn/?p=704
18.	Photo DVD Maker Professional Buffer Overflow Vulnerability	http://security.bkis.vn/?p=713

19.	ProShow Gold Buffer Overflow Vulnerabilities	http://security.bkis.vn/?p=737
20.	eoCMS SQL injection vulnerability	http://security.bkis.vn/eocms-sql-injection-vulnerability
21.	e107 Multiple Vulnerabilities	http://security.bkis.vn/e107-multiple-vulnerabilities

2.5. Others

Feb 2009: Present at BlackHat DC 2009 Conference, Washington DC, USA.
Jan 2010: Play as a scenario designer for APCERT Drill.

3. Predictions of virus situation in Vietnam in 2010

In 2010, viruses will continue to appear every day in increasingly number, especially dangerous ones such as metamorphic viruses and system files overwriting viruses. 2010 will see the proliferation of fake AV softwares targeting naive and off-guard users. Once it is getting harder in using techniques to directly attack users' computers, hackers will turn to social engineering techniques. For example, right after Microsoft released a relatively strict UAC mechanism (User Account Control), providing high level security, which grants users all the executing decisions, viruses spoofing Windows 7 notifications immediately emerged, tricking users into executing malicious code.

Mobile phones will become the new target of hackers, especially when 3G has been launched in Vietnam. In 2010, in Vietnam there will be an increase in phishing attacks and virus propagation targeting mobile phones, which has been occurring in countries with wireless broadband and advanced 3G. Attacks against mobiles can be much more dangerous than those targeting computers and Internet since users rarely take caution with the personal devices that they always get in hand. Meanwhile, with the increasing popularity of 3G, a lot of confidential and important data such as financial data, personal information, etc. are stored, updated and transacted on mobile phone.

The modified Penal Law which officially takes effect from January 01, 2010 will create a legal framework for punishing cyber-criminals spreading virus. Previously a hacker propagating virus might get financial punishment. However, according to the newly modified Penal Law, such cyber-criminals

would be subject to penal prosecution and sentenced to 1-12 month imprisonment.

3. BruCERT Activity Report

Brunei Computer Emergency Response Team - Negara Brunei Darussalam

1. About BruCERT

1.1. Introduction

Brunei National Computer Emergency Response Team (BruCERT) was established in May 2004. It was formed in collaboration with AITI, the Ministry of Communication, to become the nation's first trusted one-stop referral agency in dealing with computer-related and internet-related security incidents in Brunei Darussalam.

The Brunei Computer Emergency Response Team Coordination Centre (BruCERT) welcome reports on computer security related incident. Any computer related security incident can be reported to us by:

Telephone: (673) 2458001
Facsimile: (673) 2458002
Email: cert@brucert.org.bn

1.1.1 BruCERT Services

- 24X7 Security Related Incidents and Emergency Response from BruCERT.
- 24X7 Security Related Incidents and Emergency Response onsite (Deployment response is within 2hrs after an incident is received). This service only applies to BruCERT Constituents.
- Broadcast alerts (Early Warning) of new vulnerabilities, advisories, viruses and Security Guidelines from BruCERT Website. BruCERT Constituents will receive alerts through email and telephone as well as defense strategies in tackling IT Security related issues.
- Promote Security Awareness program to educate and increase public awareness and understanding of information security and technical know-how through education, workshop, seminar and training.
- Coordinating with other CERT, Network Service Providers, Security Vendors, Government Agencies as well as other related organization to facilitate the detection, analysis and prevention of security incidents on the internet.

1.1.2 BruCERT Workforce

BruCERT currently with strength of 44 Staff (100% local) and the rest is administration. BruCERT has undergone training on various IT security module, such as A+, N+, Linux+, Server+, Security+, SCNP, SCNA, CIW, CEH, CCNA, CISSP and BS7799 Implementer, where most of BruCERT workforce has gain certification in certain fields.

1.1.3 BruCERT Constituents

BruCERT has close relationship with Government agencies, 2 major ISPs and various numbers of vendors.

Government Agencies

Provide a security incident response services to national and government agencies as ITPSS is appointed as a central hub for all IT security-related issues across the nation and to become the Government trusted E-Security Advisor.

AITI

Authority for Info-communications Technology Industry of Brunei Darussalam (AITI) is an independent statutory body to regulate, license and develop the local ICT industry and manage the national radio frequency spectrum.

AITI has appointed ITPSS (Information Technology Protective Security Services), an IT local security company to become the national CERT in dealing with incident response in Brunei.

Royal Brunei Police Force

BruCERT has been collaborating with RBPF to resolve computer-related incidents.

TelBru – BruNet

TELBru, the main service provider of internet gateway. and BruCERT have been working together to engage information sharing of

internet-related statistics and the current situation of IT environment in Brunei.

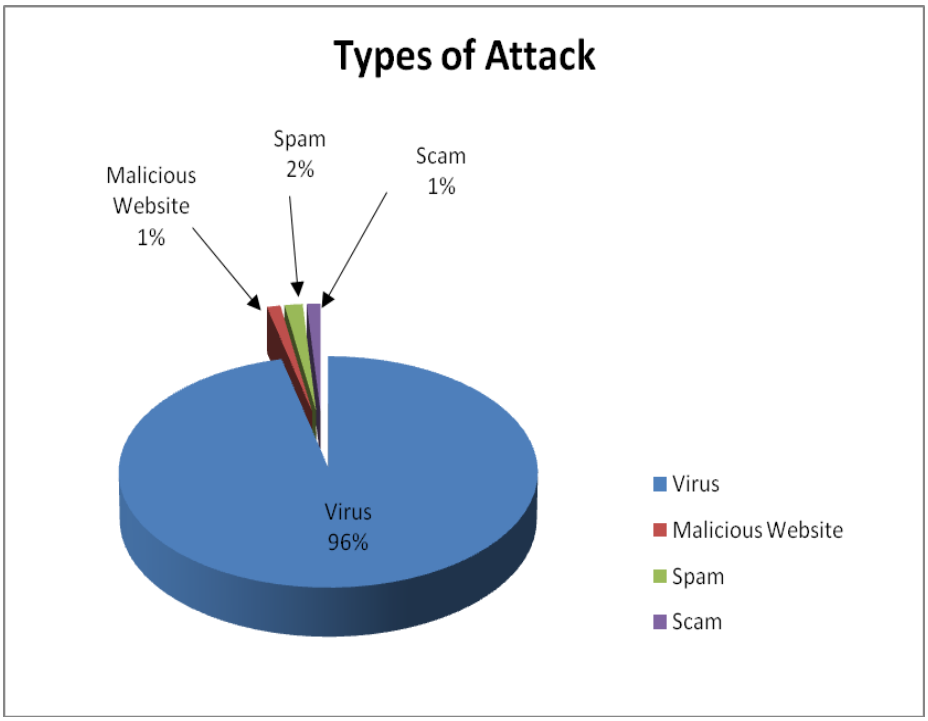
DST – simpur

The second largest internet service provider in Brunei.

2. BruCERT Activities and Operation in 2009

2.1 Incidents response

In 2009, BruCERT receive a few numbers of security incidents reports from the public even from the private sector. The most common incident report we receive is the Conficker.c virus which is widely spread in Brunei Darussalam. There were 3 incidents involving websites containing malicious code. The statistic of the security incident is shown as figure 1.



Types of Attack	Count
Virus	261
Malicious Website	3
Spam	4
Scam	3

Figure 1

2.2 New Services

BruCERT will be providing Security Monitoring Service to the Brunei Government network as part of our role in strengthening the ICT security. With this security monitoring service, it can enhance our incidents response activity and better protect our nation security in providing early warnings and advisory in a timely manner. This service is still in the implementation stage at the moment.

3. BruCERT Activities in 2009

3.1 Attended Seminars/Conferences/Meetings/Visits

BruCERT attended and presented at various seminars, conferences and meetings related to the field of ICT security.

- In 02nd March 2009 - Two BruCERT delegates attended the APCERT 2009 Annual General Meeting which takes place at Kaohsiung Taiwan.
- On May 18 2009, BruCERT participated in World Telecommunication and Information Society day celebration as a speaker providing security awareness for the public.
- In July 23rd 2009, BruCERT joined the ASEAN CERT Incident Response Drill, where the main objective is to simulate realistic cross-border incidents handling and promote collaboration among national CERTs in the region
- In June 26th 2009, Two BruCERT delegates attended the First Annual Meeting which takes place at Kyoto Japan. We also took the opportunity to visit JPCERT, NISC, JSOC and NTT-CERT
- In 19th till 23rd October 2009, Two BruCERT delegates joined the ASEAN-JAPAN workshop hosted by NISC Japan.

3.2 Training and Seminars

From January 2009 onwards, BruCERT has conducted on-going IT Security Awareness Training, at the Civil Service Institute (IPA) of Brunei Darussalam for Government Officials in three levels, which are End Users, IT personnel and Executive Management. We also provide some security awareness Training to private sector upon request.

4. Conclusion

Due to the anonymity in cyberspace, Internet crimes are getting hard to detect. In order to address these computer threats, the collaboration between BruCERT and the enforcement of various legislations together with the involvement of law enforcement agencies can help to strengthen cyber security and protect the well being of the people and nation. Besides that, collaboration among CERTs is essential in an effort to work together mitigating the risk of further incidences in the region. Its hope that BruCERT can be make known and contribute more to the public and private sector through our services.

4. CERT-In Activity Report

Indian Computer Emergency Response Team - India

1. About CERT-In

1.1. Introduction

CERT-In is a functional organisation of Department of Information Technology, Ministry of Communications and Information Technology, Government of India, with the objective of securing Indian cyber space. CERT-In provides Incident Prevention and Response services as well as Security Quality Management Services.

In the Information Technology (Amendment) Act 2008, CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
- Such other functions relating to cyber security as may be prescribed

1.2. Establishment and Constituency

CERT-In was operational since January 2004. The constituency of CERT-In is the Indian cyber community. CERT-In works cooperatively with Chief Information Officers and system administrators of various sectoral and organisational networks of its constituency.

2. Activities and Operations of CERT-In

2.1. Services and Activities

CERT-In provides:

- Proactive services in the nature of Advisories, Security Alerts, Vulnerability Notes, and Security Guidelines to help organisations secure their systems and networks

- Reactive services when security incidents occur so as to minimize damage

The summary of activities carried out by CERT-In during the year 2009 is given in the following table:

Activities	Year 2009
Security Incidents handled	8266
Security Alerts issued	29
Advisories Published	61
Vulnerability Notes Published	157
Security Guidelines Published	1
White papers/Case Studies Published	1
Trainings Organized	19
Indian Website Defacements tracked	6023
Open Proxy Servers tracked	2583
Bot Infected Systems tracked	3509166

Table 1. CERT-In Activities during year 2008

2.2. Cyber Security Assurance Framework

CERT-In has taken steps to implement National Information Security Assurance Programme (NISAP) to create awareness in government and critical sector organisations and to develop and implement information security policy and information security best practices based on ISO/IEC 27001 for protection of their infrastructure. For communicating with these organisations, CERT-In maintains a comprehensive database of more than 1000 Point-of Contacts (PoC) and Chief Information Security Officers (CISO). As a proactive measure, CERT-In has also empanelled 40 information security auditing organisations to carry out information security audit, including the vulnerability assessment and penetration test of the networked infrastructure of government and critical sector organisations. The technical competency of the empanelled orgnanisations is regularly reviewed by CERT-In with the help of a test network.

CERT-In also conducted a cyber security mock drill to assess the preparedness of organizations in the critical sector to withstand cyber attacks.

CERT-In plays the role of mother CERT and is regularly interacting with the cyber security officers of sectorial CERTs in Defense, Finance and other sectors to advise them in the matters related to cyber security.

To facilitate its tasks, CERT-In has collaboration arrangements with IT product vendors, security vendors and Industry in the country and abroad. This collaboration facilitates exchange of information on vulnerabilities in relevant products, developing suitable countermeasures to protect these systems and providing training on latest products and technologies.

CERT-In in collaboration with CII, NASSCOM and Microsoft have created a portal "secureyourpc.in" to educate consumers on cyber security issues.

2.3. Incident Handling Reports

2.3.1. Summary of Computer Security Incidents handled by CERT-In during 2009

In the year 2009, CERT-In handled more than 8000 incidents. The types of incidents handled were mostly of Phishing, Malicious Code, Website compromise & propagation of malware and Network Scanning & Probing.

The year-wise summary of various types of incidents handled is given below:

Security Incidents	2004	2005	2006	2007	2008	2009
Phishing	3	101	339	392	604	374
Network Scanning / Probing	11	40	177	223	265	303
Virus / Malicious Code	5	95	19	358	408	596
Spam	-	-	-	-	305	285
Website Compromise & Malware Propagation	-	-	-	-	835	6548
Denial of Service	-	-	-	-	54	15
Others	4	18	17	264	94	145
Total	**23**	**254**	**552**	**1237**	**2565**	**8266**

Table 2. Year-wise summary of Security Incidents handled

2.3.2. Incident Statistics

Various types of incidents handled by CERT-In are given in Figure 1.

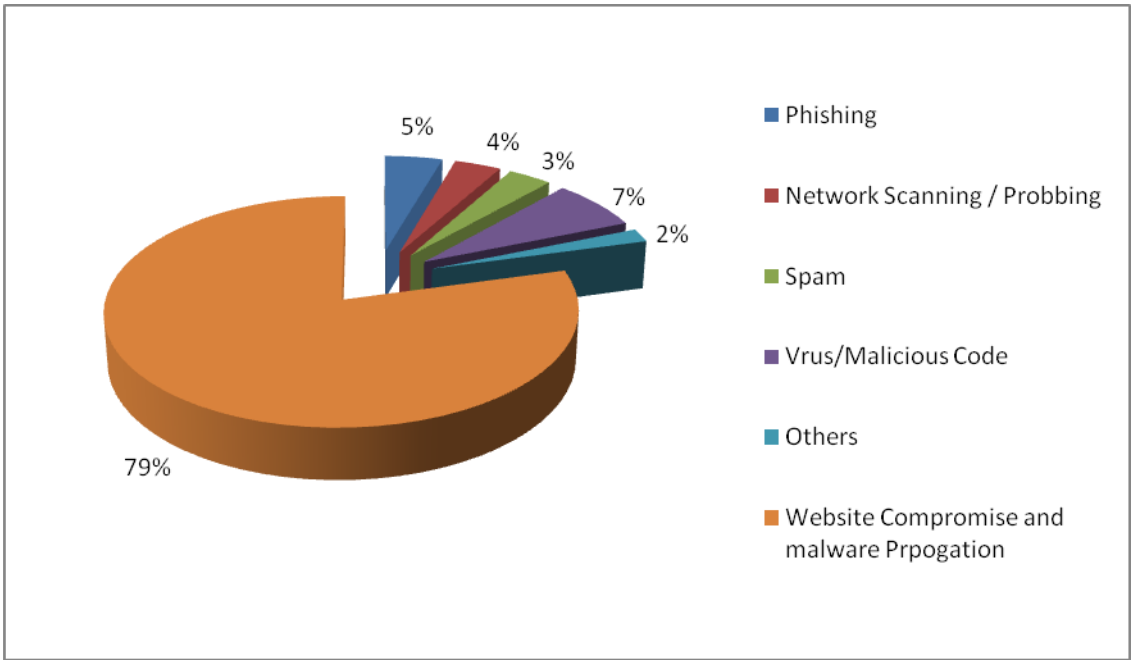


Figure 1. Summary of incidents handled by CERT-In during 2009

2.3.3. Incident Trends

During the year 2009 CERT-In handled several incidents of intrusions into websites and injecting iFrame and Java script to redirect visitors to malicious websites. By exploiting vulnerabilities such as SQL injection and XSS flaws, trusted websites are converted to malicious websites serving content that contains client side exploits

CERT-In has observed that commonly used programs such as Adobe PDF Reader ,Adobe Flash and Microsoft office are exploited widely to steal data from the target computers and also to install back doors through which the attackers can gain control for further exploitations.. Also there has been an increase in the number of Zero Day Vulnerabilities.

It has been observed that the Koobface worm propagating through social networking sites such as Facebook, MySpace, hi5, Bebo, Friendster and Twitter etc.

It is reported that a stealth worm "Psybot" targeting home routers and DSL modems are in the wild. The worm infects any of a family of Linux Mipsel devices that contain one of several administration interfaces.

It has been reported that Worm:iPhoneOS/Ikee and variants - the first worm to target the Apple iPhone- are in the wild spreading using the default root password in SSH among jail-broken iPhones.

Incidents of stealing of user credentials due to infection of client systems by Zeus and Clampi botnets were on the rise. Various variants of Win32/Zbot , part of Zeus botnet , observed.

Incidents of malicious domains such as Gumblar that was hosting the malware exploit , has been actively used for compromising thousands websites. It is a drive by download with multiple stages. The first stage of exploit is to attempt to inject malicious code onto the vulnerable website primarily through stolen FTP credentials, poor configuration settings, vulnerable web application etc.

Propagation of malware through new and innovative techniques such as impersonation of "mail administrator" etc were noticed.

The Conficker worm which transpired in November 2008 was propagating widely till May 2009 infecting large number of systems in India.

2.4. Proactive Services

2.4.1. Tracking of Indian Website Defacements

CERT-In has been tracking the defacements of Indian websites and suggesting suitable measures to harden the web servers to concerned organizations. In all 6023 numbers of defacements have been tracked. Most of the defacements were done for the websites under .in domain. In total 3042 .in domain websites were defaced.

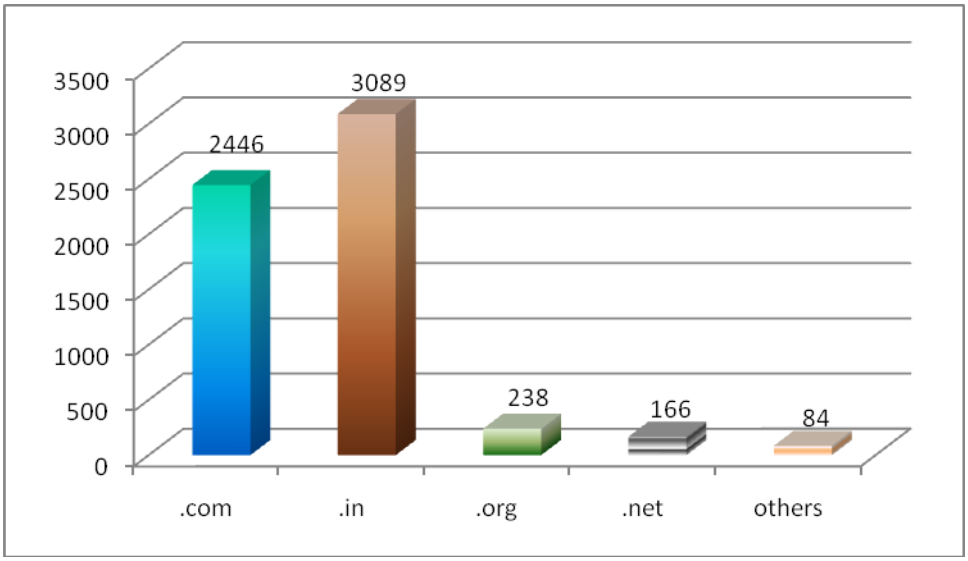


Figure 2. Indian websites defaced during 2009 (Top level domains)

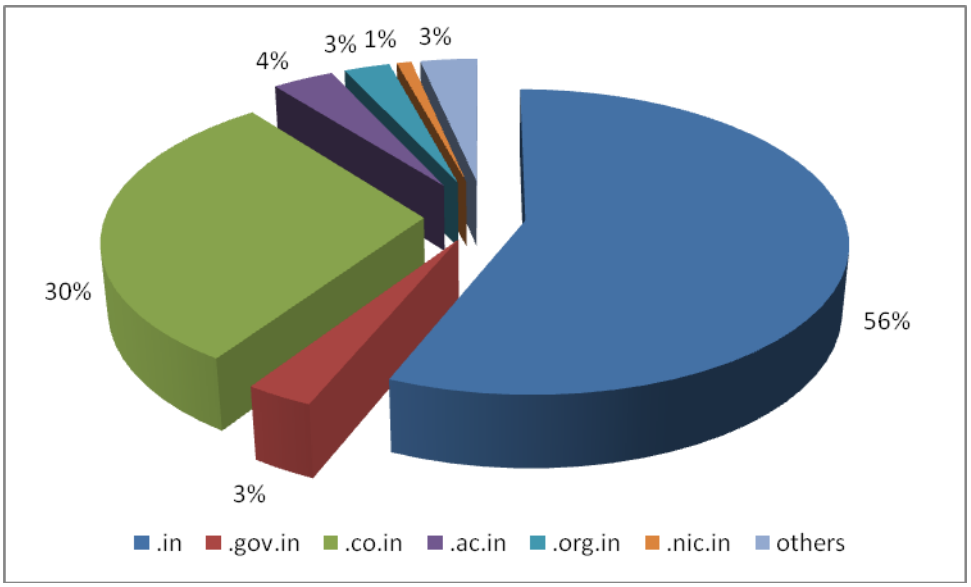


Figure 2.1 .in ccTLD defacements during 2009

2.4.2. Tracking of Open Proxy Servers

CERT-In is tracking the open proxy servers existing in India and proactively alerting concerned system administrators to properly configure the same in order to reduce spamming and other malicious activities originating from India. In all 2583 open proxy servers were tracked in the year 2009. The month-wise distribution of open proxy servers tracked during this year is shown in the figure 3.

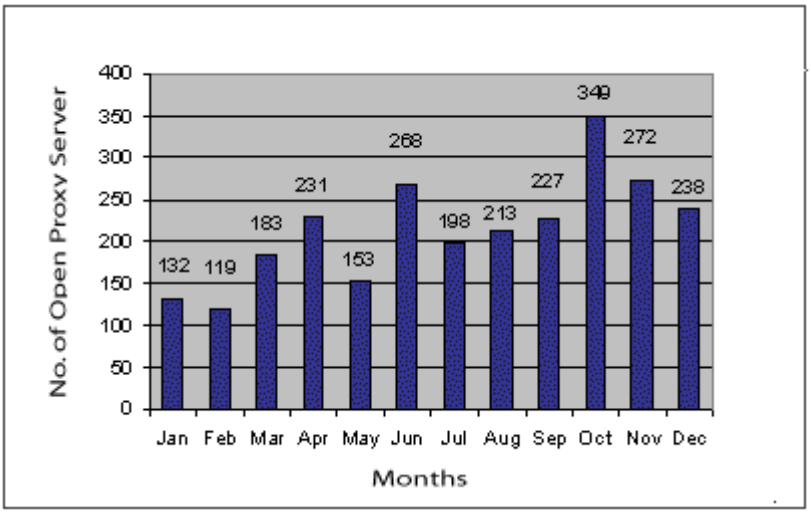


Figure 3. Monthly statistics of Open Proxy Servers in 2009

2.4.3. Botnet Tracking and Mitigation

CERT-In is tracking Bots and Botnets involving Indian systems. After tracking the IP addresses of Command and Control servers and Bots operating within India, actions are being taken to clean the respective systems and prevent malicious activities. Figure 4 shows the number of Bot infected systems and Command & Control servers tracked in 2009.

Month	Number of Bot Infected Systems	C&C Servers
January	277697	5
February	590362	07
March	30,025	02
April	1495485	07
May	4, 53,076	07
June	68,824	10
July	28854	-
August	188295	-
September	202478	-
October	96114	-
November	49759	18
December	28197	-

Figure 4. Botnet statistics in 2009

3. Events organized / co-organized

3.1. Education and Training

To create awareness and to enable users to implement best practices, CERT-In is organizing workshops and training programmes on focused topics for targeted audience such as CISOs, financial and banking sector officers, System Administrators, ISPs etc. Experts from industry are delivering lectures in these workshops apart from CERT-In staff. CERT-In has conducted the following training programmes during 2009.

- Workshop on" Linux Security" on December 17-18, 2009
- Workshop on" Secure Code Review for PHP Applications" on December 08, 2009
- Workshop on " Secure Coding in PHP: Developing Defensive Applications " on December 07, 2009
- Workshop on "Secure Code Review for JAVA Applications" on November 20, 2009
- Workshop on "Developing Secure Code in JAVA" on November 06, 2009
- Workshop on " Database Server Security" on October 14, 2009
- Workshop on " Advanced Web Application Security" on September 23, 2009
- Workshop on " Computer Forensics " on August 27-28, 2009
- Workshop on " Threat Infiltration and Mitigation " on August 3, 2009
- Workshop on "Defending Phishing Attacks" on July 30, 2009
- Workshop on " Identity and Access Management " on July 24, 2009
- Workshop on "Web Application Security – Current Trends" on July 3, 2009
- Workshop on "Windows Security" on June 26, 2009
- Workshop on "Wireless Security" on May 28-29, 2009
- Workshop on "Critical Information Infrastructure Resiliency" on May 19-21, 2009
- Workshop on "Application Code Security Review" on March 25, 2009
- Workshop on "Development of Secure Code guidelines for .NET" on March 18, 2009
- Workshop on " Web Application Security : Advanced Topics" February 09, 2009
- Workshop on "Application Security : Latest Trends" , January 30, 2009

3.2. Forums

CERT-In is collaborating with National Association of Software & Service Companies (NASSCOM) and Data Security Council of India (DSCI) to spread the cyber security awareness and facilitate interaction with various user groups.

4. Achievements

4.1. Publications

The following were published by CERT-In in the year 2009:

1. Paper titled “cyber terrorism: current threats and challenges” (52nd Annual Technical Convention on TECHNOLOGY AND TERROR role of ICT in war against terror September 26-27,2009 conducted by IETE) . This paper examines the current threats of cyber terrorism and methods of cyber criminals. The challenges in combating the cyber threats and possible solutions are highlighted from the technical and social perspective.
2. Series of Mass iframe Injection on Websites-Serving Blended Malware (CICS-2009-01). It has been observed that thousands of websites have been compromised and infected with iframe script tags linking users to malicious JavaScript file hosted on domain " a0v [d0t] org ". It has been found that most of the websites running in support of ASP engine are infected. Details of multiple redirections and infection is illustrated in CERT-In Case Study CICS-2009-01.
3. Survey "State of Data Security and Privacy in the Indian Industry" conducted in association with Data Security council of India (DSCI). This is an attempt to assess the preparedness of Indian organizations in IT and IT enabled services facing the challenge of securing their IT infra structure. The results of the survey showed that information security is getting its due priority among majority of enterprises in the country.
4. Monthly security bulletins: Monthly security bulletin comprises of Statistics of incidents handled by CERT-In, information on vulnerabilities in various operating systems and applications tracked, Cyber intrusion trends and other relevant IT security issues.

5. International Collaboration

CERT-In has established collaborations with international security organisations and CERTs to facilitate exchange of information related to latest cyber security threats and international best practices. CERT-In is a member of Forum of Incident Response and Security Teams (FIRST), APCERT and Anti-Phishing Working Group (APWG).

5.1. Drills

- CERT-In has successfully participated in ASEAN CERTs Incident Handling Drill (ACID 2009) held in July 2009 involving CERTs from Asia Pacific region and Europe.

6. Future Plans/Projects

CERT-In has been evolved as the most trusted referral agency in the area of information security in the country. Following are the future plans:

- Regular interaction with CISOs of Critical Infrastructure Organisations and sectorial CERTs to ensure security of the critical systems.
- Development and implementation of a framework to enable organisations to respond to cyber incidents and assess the preparedness of organisations to withstand cyber attacks
- Collaboration with IT product and security vendors to mitigate the vulnerabilities in various systems and cooperation with international CERTs and security organizations on information sharing and incident response
- Promotion of R&D activities in the areas of attack detection & prevention and Cyber Forensics

5. CNCERT/CC Activity Report

National Computer network Emergency Response technical Team/Coordination Center of China - People's Republic of China

1. About CNCERT

1.1 Introduction

CNCERT is a National level CERT organization, which is responsible for the coordination of activities among all CERTs within China concerning incidents in national public networks.

1.2 Establishment

CNCERT was founded in Oct., 2000, and became a member of FIRST in Aug., 2002. CNCERT took an active part in the establishment of APCERT as a founding member.

1.3 Workforce power

CNCERT, which is headquartered in Beijing, the capital of P.R.China, has 31 provincial branch offices in 31 provinces of China mainland.

1.4 Constituency & Etc

CNCERT provides computer network security services and technology support in the handling of security incidents for national public networks, important national application systems and key organizations, involving detection, prediction, response and prevention. It collects, verifies, accumulates and publishes authoritative information on the Internet security issues. It is also responsible for the exchange of information, coordination of action with International Security Organizations.

CNCERT's activities are:

Information Collecting	collect various timely information on security events via various communication ways and cooperative system
Event Monitoring	detect various highly severe security problems and events in time, and deliver precaution and support

	for the related organizations.
Incident Handling	leverage domestic CERTs to handle various public network security incidents, and act as a premier window to accept and handle incident reports from homeland and world.
Data Analyzing	conduct comprehensive analysis with the data of security events, and produce trusted reports.
Resource Building	collect and maintain various basic information resources, including vulnerabilities, patches, defending tools and latest network security technologies for supporting purpose.
Security Research	research on various security issues and technologies as the basic work for security defense and emergency response.
Security Training	provide training courses on emergency response and handling technologies and the construction of CERT.
Technical Consulting	offer various technical consulting services on security incident handling.
International Exchanging	organize domestic CERTs to conduct international cooperation and exchange.

CONTACT

E-mail: cncert@cert.org.cn

Hotline: +8610 82990999 (Chinese), 82991000 (English)

Fax: +8610 82990375

PGP Key: http://www.cert.org.cn/cncert.asc

2. Activities & Operations

2.1 Incident handling reports

In 2009, CNCERT received 21,927 incidents reports from domestic and international users and agencies. Most incident reports were about spam mail (67.38%), webpage embedded malicious code (22.39%), and phishing (5.47%).

In 2009, CNCERT handled 1,125 incidents. Webpage embedded malicious code (462), phishing (293) and web defacement (273) were 3 main incidents handled.

TOP 10 Phishing Victim

Organization	Number
ebay/paypal	298
HSBC	97
BBVA	54
BANCO BRADESCO S.A.	29
commonwealth bank of Australia	28
facebook	24
citibank	22
Westpac Banking Corporation	21
Internal Revenue Service	18
Twitter	17

TOP 10 Phishing Reporters

Organization	Number
ebay/paypal	269
auscert.org.au	130
HSBC	95
markmonitor.com	95
s21sec.com	69
cyf-kr.edu.pl	67
Cyveillance.com	52
rsa.com	50
melbourneitdbs.com	31
brandprotect.com	27

2.2 Abuse Statistics

Traffic Monitoring and Analysis

According to CNCERT's data of Internet traffic sample monitoring, the top 5 applications of TCP traffic are among HTTP, P2P and email.

TCP Port	Rank	Percentage	Applications
80	1	19.48%	HTTP
443	2	1.14%	Https
4662	3	1.07%	eMule
25	4	0.71%	SMTP
8080	5	0.64%	HTTP
1863	6	0.42%	MSN Messenger
3128	7	0.37%	HTTP
1935	8	0.37%	RTMP
554	9	0.16%	RTSP
1755	10	0.14%	MMS

TCP Traffic Top 10 in 2009

The top 3 applications of UDP traffic were Xunlei, MSN and QQ.

UDP Port	Rank	Percentage	Applications
15000	1	3.21%	Xunlei (downloader)
1863	2	1.25%	MSN
29909	3	1.20%	QQ(downloader)
8000	4	1.15%	QQ IM
7600	5	0.86%	Unknown
8889	6	0.56%	P2P downloader
80	7	0.44%	Http
21871	8	0.39%	P2P downloader
8183	9	0.36%	P2P downloader
7100	10	0.34%	Online Game

UDP Traffic Top 10 in Year 2009

Trojan & Botnet Monitoring

In 2009, CNCERT organized a few special actions of crack down on Trojan & Botnet C&C server, which resulted in successful effectiveness. 262,419 IP addresses of computers embedded with Trojans were discovered in Chinese mainland, decreased by 53.6% compared with that of year 2008. 837,296 IP addresses of computers embedded with bot discovered in Chinese mainland decreased by 32.3% compared with that of year 2008.

Meanwhile, 18,640 C&C servers outside of Chinese mainland were discovered controlling bots in Chinese mainland. Among these C&C servers, 22.34% were in the United States, 8.26% in Mexico and 7.47% in India.

In general, the size of Botnets is going on to become smaller, localized and specialized. The Botnet with less than 1,000 bots is much more favorable to attackers.

Conficker Monitoring

At the end of 2008, Conficker worm began to spread around the world with multiple variants. Variants B and C are most active ones. By April 30, 2009, there were more than 7.84 millions of IP addresses of computer infected in the world, of which China mainland ranked first, accounting for 20.82%.

In second half of 2009, the proportion of number of computers infected with Conficker worm in China mainland declined slightly in the world, but the absolute number remain high. The monthly average number is more than 18 million IP addresses of computers infected in China mainland.

Web Defacement Monitoring

In 2009, CNCERT discovered about 42,000 defaced websites in China mainland, which decreased by about 1/5 compared with that of year 2008. 1,994 are governmental websites, a relative large proportion.

2.3 New services

In 2009, CNCERT promoted its information services to a wider users group and a richer categories choice. CNCERT developed more partners and provided them with customized information. Besides existing security bulletins, vulnerability advisories, malware warnings, technical reports, security guide, monthly report, and annual report, more information services were created to be delivered to users, like weekly report, monthly Internet security index report, weekly vulnerability report, and etc.

3. Events organized/co-organized

3.1 Training

N/A

3.2 Drills

MIIT 2009 Drill, co-organized with MIIT.

APCERT 2010 Drill, as the organizing committee member with HKCERT and MyCERT.

ACID 2009, CNCERT participated in ACID 2009 on 30th July 2008

3.3 Seminars & Etc

Seminar on 2 New MIIT Regulation Drafts

The Seminar was held in Beijing, April 2009. The regulation drafts of "Internet Network Security Information Notification Implementation Measures" and "Trojans and Botnet Monitoring and Handling Mechanism" were discussed in the seminar for officially release readiness.

Kick Off Meeting of Network Anti-virus Alliance

The meeting was held in Beijing on 7 July 2009. The “Network Anti-virus Self-regulation Convention” was signed by all participating members, including ISPs, domain name registrars, security vendors and etc. The Alliance was initiated to be founded by CNCERT to keep down network virus and clean up the Internet environment.

Kick Off Meeting of CNVD Project

The meeting was held in Changsha on 22 Oct 2009. The cooperative agreement was signed by all participating members, including security vendors, software vendors, Internet forms and etc. The project was initiated by CNCERT for a sharing platform of national information security vulnerability.

CNCERT 2009 Annual Conference

The Conference was held in Changsha from 21 to 24 Oct 2009. Over 300 delegates from 10 countries and regions attended the conference.

China-ASEAN Network Security Seminar

The Seminar was held in Changsha on 23rd Oct 2009. 13 delegates from 7 ASEAN member countries attended the meeting.

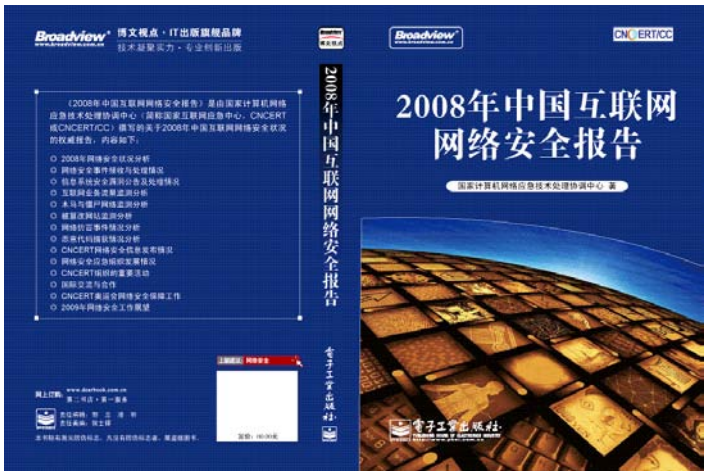
4. Achievements

4.1 Presentation

Network Security Assistance to the Beijing Olympics, 21st Annual FIRST Conference, 2009.6.28-7.3, Kyoto, Japan.

Issues and Cases of Internet Misuse in China, APEC Training Program Meeting, 2009.8.31-9.1, Seoul, Korea

4.2 Publication



"2008 China Internet Security Report" (in Chinese, ISBN: 978-7-121-08723-3).

4.3 Certification & Etc

In 2009, CNCERT renewed its ER service partners with service-level certification. 10 vendors were certified with CNCERT National-level ER Service Partner; 12 vendors were certified with CNCERT Regional-level ER Service Partner; 33 vendors were certified with CNCERT Provincial-level ER Service Partner.

5. International Collaboration

5.1 MoU

N/A

5.2 Conferences and Events

21st Annual FIRST Conference

CNCERT delegation attended the FIRST Conference in Kyoto, Japan, 2009.6.28-7.3.

ACID 2009

CNCERT participated in the ACID 2009, 2009.7.23.

Meeting with CERT-Hungary

CNCERT had a meeting with CERT-Hungary in Hungary, 2009.4.1-4.9

Meeting with TWCERT

CNCERT had a meeting with TWCERT in Taiwan, China, 2009.8

6. Future Plans

6.1 Future projects

N/A

6.2 Framework

6.2.1 Future operation

As usual.

6.2.2 Tracking

Conficker worm monitoring

6.3 Etc

CNCERT will be prepared for network security assurance for **EXPO 2010** from May 1 to Oct 31, 2010 in Shanghai and the **16th Asian Games** from Nov. 12-27, 2010 in Guangzhou. Therefore, we expect to keep a stronger collaboration with APCERT members then.

7. Conclusion

In 2009, CNCERT implemented a total of five times of special action and removed more than 1,200 command & control servers and malicious domain names used by Trojans and Botnets, so the Internet environment got to be cleaned up further. 511 event of China Telecom DNS service down really

caused a lot of serious concern, but the related work like basic DNS infrastructure building, collaboration mechanism consolidation, online application software security promotion and etc got to be driven to move forward accordingly.

6. HKCERT Activity Report

Hong Kong Computer Emergency Response Team Coordination Centre - Hong Kong, China

1. About HKCERT

1.1 Establishment

- Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) was established in 2001 with funding from the Hong Kong Special Administrative Region (HKSAR) Government. The Hong Kong Productivity Council (HKPC), which is a government subvented organization in Hong Kong, has operated the centre since then.

1.2 Mission and Constituency

- HKCERT is the centre of coordination of computer security incident response for local enterprises and Internet users in Hong Kong. Her missions are to handle computer security incident reports, gather and disseminate information relating to security issues, advise on preventive measures against security threats, promote information security awareness, and maintain network with other computer emergency response teams (CERT) and security organizations to facilitate coordination and collaboration.

1.3 Organization

- The senior management of HKPC oversees the overall direction and operation of the centre. The daily operations are taken care by the Centre Manager, two consultants and a group of computer security specialists

2. Operations and Activities

2.1 Incident Handling

- During the period from January to December of 2009, HKCERT had handled 1304 incidents, including 337 virus incidents, 961 security incidents and 6 other incidents. Security incident reports continue to overtake virus incident reports (See Figure 1). In addition, the number of incidents identified through proactive discovery has also increased.

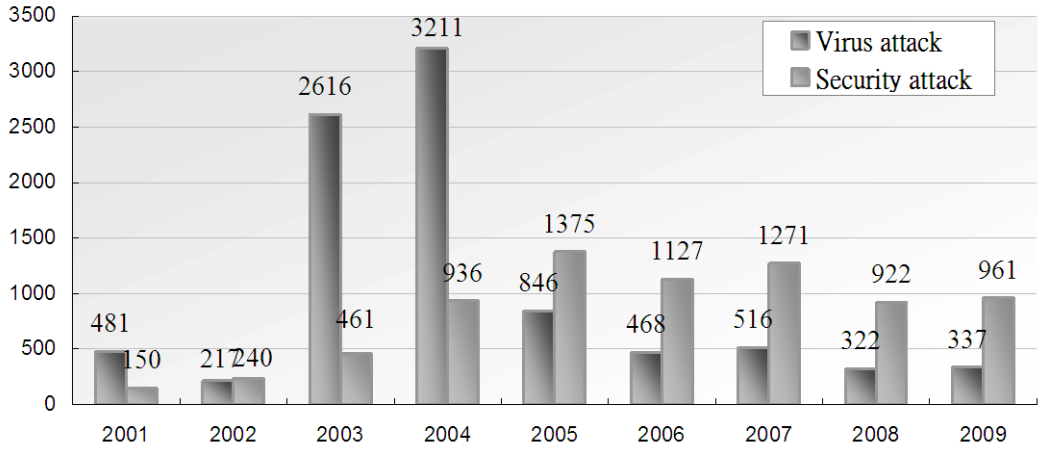


Figure 1. HKCERT Incident Reports in 2009

2.2 Information Gathering and Dissemination

- During the period from January to December of 2009, HKCERT published 220 security vulnerability alerts and advisories. No malware alert was published during this period.

2.3 Publications

- We had published 12 issues of e-Newsletter and sent out alert summaries twice per month.

3. Security Awareness and Training

3.1 Seminars, Conference and Meetings

- HKCERT jointly organized the Hong Kong Clean PC Day 2009 campaign with the Government and Police. The campaign involved public seminars, ISP symposium and an online story writing competition.
- We organized the Information Security Summit 2009 with other organizations and associations in November 2009, inviting local and international speakers to provide insights and updates to local corporate users.

3.2 Training

- We have assisted the organization of the technical training workshops of the Information Security Summit and coordinated two overseas experts to deliver hands-on workshops on “Monitoring and Analyzing Web Client Side Attacks”.

3.3 Speeches and Presentations

- HKCERT was invited to deliver speeches and presentations on various occasions for Government, associations and schools. We were also interviewed by the media from time to time to give objective and professional views on information security topics and incidents.

4. Coordination and collaboration

4.1 International Collaboration

- Participated in the Microsoft Security Cooperation Program to share information
- Represented APCERT in the Advisory Council of DotAsia.
- Joined the Tsubame distributed honeypot project of JPCERT/CC.
- Participated in the APCERT AGM and Conference and elected as the chair of APCERT.
- Participated in the APEC TEL Working Group meeting held in Singapore and delivered a speech, as the chair of APCERT, on Conficker Worm.
- Participated in the FIRST AGM and Conference and the Collaboration Meeting for CSIRT with National Responsibility organized by CERT/CC.
- Participated in the APCERT Drill on 28 January 2010 -- HKCERT took leadership in scenario preparation and acted as the EXCON. The drill was a great success.

4.2 Local Collaboration

- Provided cyber security assurance services to the East Asian Game held in Hong Kong in December 2009.
- Coordinated meetings pertaining to the Conficker worm
- Continued to work closely with the government and law enforcement agency, and held meetings to exchange information and to organize joint events regularly
- Continued to work with police, ISPs and domain registries on closing down bulletproof hosting, phishing sites and botnet command and control centres in Hong Kong
- Organized a local drill on 16 July 2009 and got some critical information infrastructure and ISPs involved. HKCERT prepared the scenarios and acted as the EXCON of the drill. The drill was a great success.

- Participated in the government's Information Infrastructure Liaison Group and Information Security Task Force
- Met with the Macao CERT in her startup stage to foster closer collaboration and exchange of information.

5. Other Activities

5.1 Third party service review

- HKCERT had carried out a third party review on the operations and services in November 2009 as requested by the government. JPCERT/CC was invited as the reviewer. The review covered the core operations and services, publication, organizational relationships, supporting organization, information management and human resources. Recommendations were made on the enhancing the services and coping with the future trends.

6. Future Plans

- HKCERT has secured Government funding to provide the basic CERT services starting from 2009. We shall work closely with the government to plan for the future services of HKCERT.
- We shall plan on implementing the recommendations proposed in the third party review.
- We shall continue to propose new initiatives to the government and seek support from the government.
- We shall continue to work closely with local ISPs and Domain Name Registries, to enhance our capability in proactive security incident discovery and malware analysis.
- We shall revamp our web site and improve our internal systems to support the changing environment of our Computer Emergency Response Services.

7. JPCERT/CC Activity Report

Japan Computer Emergency Response Team/Coordination Center - Japan

1. About JPCERT/CC

1.1 Establishment

JPCERT/CC is the first CSIRT (Computer Security Incident Response Team) established in Japan. It is an independent non-profit organization, serving as a national point of contact for the CSIRTs in Japan and worldwide. After its inception in 1992, JPCERT/CC was officially established in 1996, and has been conducting incident handling operations, vulnerability handling operations, engaging in malware and threat analysis, publishing security alerts and advisories to the wide public, organizing forums and seminars to raise awareness of security issues, and supporting the establishment and operations of CSIRTs in Japan and overseas.

1.2 Constituency

JPCERT/CC coordinates with network service providers, security vendors, government agencies, as well as the industry associations in Japan.

2. Activities & Operations

2.1 Incident Handling Reports

In 2009, JPCERT/CC received 6,792 reports on computer security incidents from Japan and overseas. A ticket number is assigned to each incident report to keep track of the status.

	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	Total
Incident Reports	564	1197	2983	2048	**6,792**

Figure 1. Incident reports to JPCERT/CC (2009)

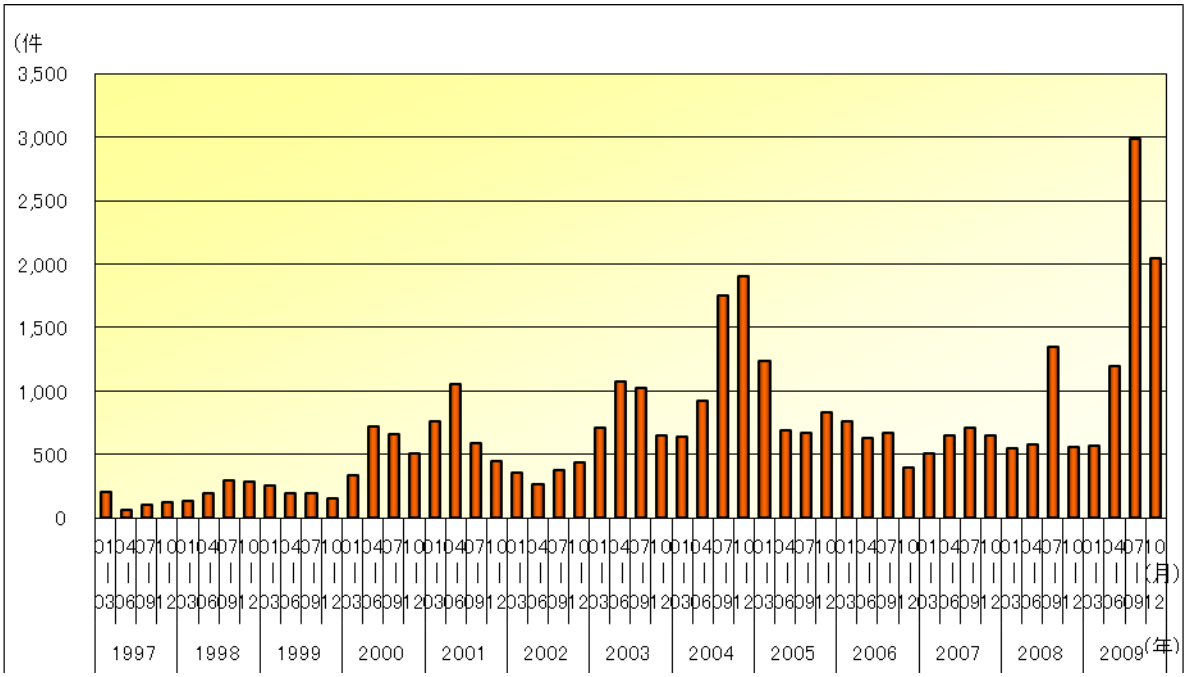


Figure 2. Incident reports to JPCERT/CC (1997-2009)

2.2 Abuse statistics

The incident reports to JPCERT/CC in 2009 were categorized as in Figure 3. More than half of the incident reports were on malware, followed by scan, phishing and intrusion.

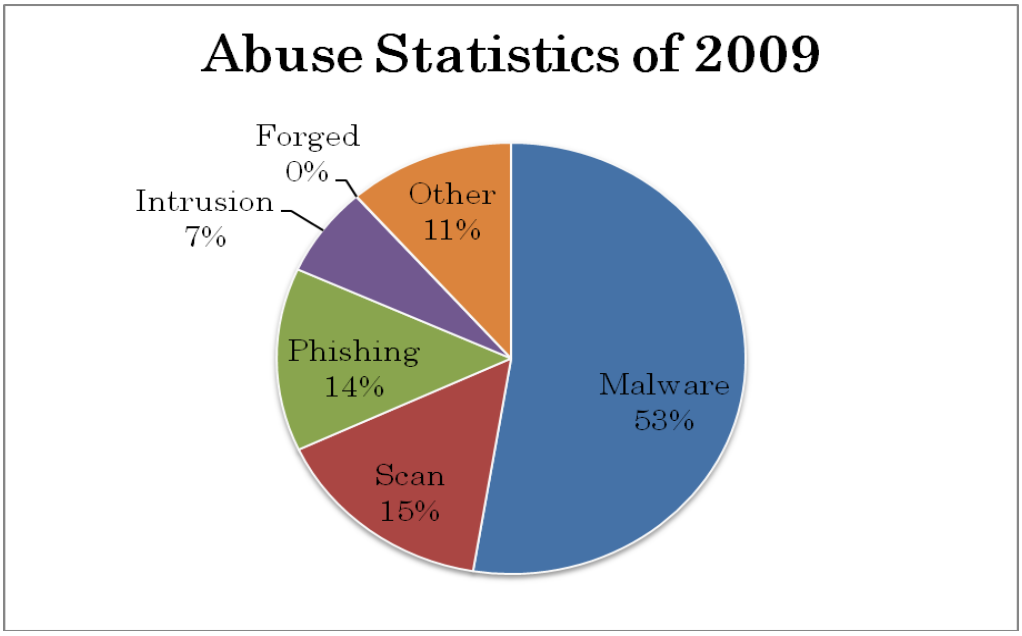


Figure 3. Abuse Statistics of 2009

2.3 Security Alerts and Advisories

Security Alerts

https://www.jpcert.or.jp/english/

JPCERT/CC publishes security alerts on widespread, emerging, information security threats and their solutions, on an as-needed basis.
In 2009, 33 security alerts were published.

Early Warning Information

JPCERT/CC publishes early warning information to the government and to organizations providing national critical infrastructure services and products. Early warning information contains information on threats, threat analysis and their solutions.

Japan Vulnerability Notes (JVN)

http://jvn.jp/en/

JVN is a vulnerability information portal site that provides vulnerability information and their solutions for software products used in Japan. JVN is operated jointly by JPCERT/CC and the Information-technology Promotion Agency (IPA) and provides the descriptions, solutions, and developers' statements (including information on affected products, workarounds and solutions, such as updates and patches) on each vulnerability.

JPCERT/CC conducts vulnerability handling operations cooperatively with CERT/CC (http://www.cert.org/), CPNI (http://www.cpni.gov.uk/) and CERT-FI (http://www.cert.fi/en/).

In 2009, 143 vulnerabilities coordinated by JPCERT/CC were published on JVN. Among them 79 cases were reported through IPA in Japan, and 64 cases were published in cooperation with CERT/CC.

JPCERT/CC Weekly Report

JPCERT/CC publishes weekly reports on selected security information of the preceding week that is regarded as high importance by JPCERT/CC. Weekly reports also contain a relevant security tip every week.

2.4 Control System Security

JPCERT/CC coordinates control system security with relevant organizations in Japan. It provides information on vulneravilities and solutions on control systems, lists of recommended reading materials, as well as reports and documents.

2.5 Learnings

Secure Coding

JPCERT/CC provides C/C++ secure coding seminars, CERT C Secure Coding Standards, books and materials on secure software development and secure coding rules.

Techinical Notes

JPCERT/CC publishes documents that provide general technical information and/or instructions for incident handling.

Library

The library provides security materials targeting both security professionals and beginners, such as information security materials for new employees, security setup of e-mail software, professional security review, etc.

2.6 Internet Scan Acquisition System (ISDAS)

http://www.jpcert.or.jp/isdas/index-en.html

ISDAS monitors the Internet traffic in Japan in order to detect threat activities such as worm and scan. The project initiated in November 2003 with the objective to improve the Internet security by providing up-to-date graphs and reports.

2.7 TSUBAME (Internet Threat Monitoring Data Sharing Project)

TSUBAME project is to collect, share and analyze Internet traffic data, in order to understand the Internet threat situation in the Asia Pacific region. It

deploys sensors widely in the region and collects/shares the data with all participating teams. TSUBAME project is aimed to establish a common platform to promote collaboration among CSIRTs in the Asia Pacific region.

2.8 Associations , Projects and Communities

Nippon CSIRT Association

The association is a community for CSIRTs in Japan. There are currently 15 member teams, and JPCERT/CC serves as the secretariat.

Cyber Clean Center (CCC)

https://www.ccc.go.jp/en_index.html

CCC is active in analyzing characteristics of BOTs, and providing information on disinfestation of BOTs from users' computers. In addition, CCC is a core organization taking a role to promote BOT cleaning and prevention of re-infection of users' computers which are once infected by BOTs, based on cooperation with ISPs (Internet Service Providers).
CCC is a project coordinated by the Ministry of Internal Affairs and Communications (MIC) and Ministry of Economy, Trade and Industry (METI). JPCERT/CC contributes to the project by analyzing malware and developing disinfestation tools for infected users.

Council of Anti-Phishing Japan

JPCERT/CC serves as the secretariat for the Council of Anti-Phishing Japan.

3. Events organized / co-organized

3.1 Trainings and Seminars

JPCERT/CC offers trainings, seminars and workshops, for technical staffs, system administrators, network managers, etc. Some of the events organized or co-organized by JPCERT/CC in 2009 are as follows:

- C/C++ Secure Coding Seminars
- CSIRT Training Course (4th - 12th February 2009)
- Control System Security Conference 2009 (18th - 19th February 2009)
- Critical Information Infrastructure Protection Security Forum 2009 (20th February 2009)
- 21st Annual FIRST Conference Kyoto (28th June - 3rd July 2009)

- Internet Week 2009 (24th November 2009)
- Security Day 2009 (16th December 2009)

3.2 Drills

JPCERT/CC participated in the following drills:

- ASEAN CERT Incident Drill (ACID) 2009
- APCERT Drill 2010

4. Other Publications

JPCERT/CC also publishes quarterly activity reports, study/research reports, and CSIRT related materials.

5. International Contribution

FIRST (Forum of Incident Response and Security Teams)

http://www.first.org

JPCERT/CC contributes to the international CSIRT community by serving as a Director and Steering Committee member of the FIRST organization, since 2005.

ISO International Standard
(ISO/IEC JTC 1/SC 27 Information technology – Security techniques)

JPCERT/CC contributes to the following ISO Internation Standards being developed under ISO/IEC JTC 1/SC 27:

- ISO/IEC 29147: "Responsible Vulnerability Disclosure"
- ISO/IEC 27035: "Information Security Incident Management"

JPCERT/CC Contact Information

URL: http://www.jpcert.or.jp/
E-mail: info@jpcert.or.jp
Phone: +81-3-3518-4600
Fax: +81-3-3518-4602

8. KrCERT/CC Activity Report

Korea Internet Security Center - Korea

1. About KrCERT/CC

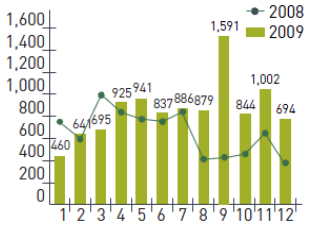
KrCERT/CC, also known as KISC, Korea Internet Security Center, serves as the nationwide Internet incident handling and coordination center in Korea, and is responsible for detecting, analyzing and responding all nationwide Internet incidents such as hacking, worm/virus, bot, phishing, and all other various Internet threats. To mitigate the damage from those incidents occurred and to ensure more secure Internet environment, KrCERT/CC is seamlessly operating on 24/7 basis.

2. Internet Incident Statistics and Analysis

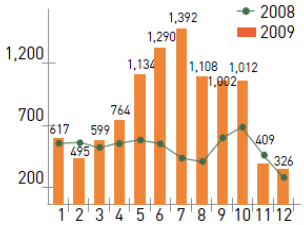
2.1. Overview

Internet incident reports received by the KrCERT/CC are categorized into worm/virus, hacking incident, and bot. Hacking incident has subcategories; spam relay, phishing[1], intrusion attempt, webpage defacement, and other. The number of malicious code reported to KrCERT/CC in 2009 is 10,395, which is 23% increase compared with that of the last year (8,469 in 2008). The number of hacking incident reported to KrCERT/CC in 2009 is 21,230, which has 33% increase compared with that of the last year (15,940 in 2008).

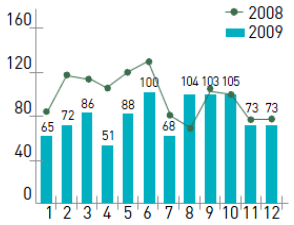
Worm/Virus



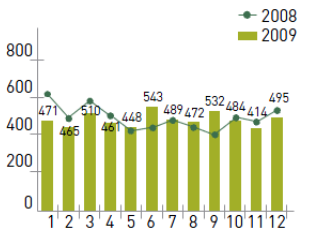
Spam Relay



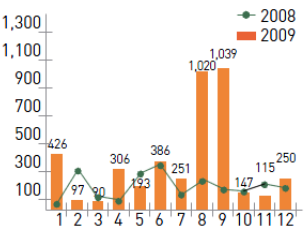
Phishing Host



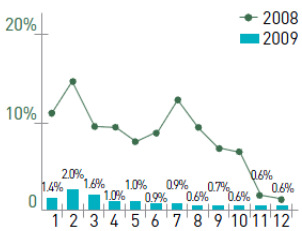
Intrusion + Other



Web Defacement



Bot Infection



[1] Phishing targeting Korean brands is very rare; however, many Korean websites are abused as phishing host targeting foreign brands.

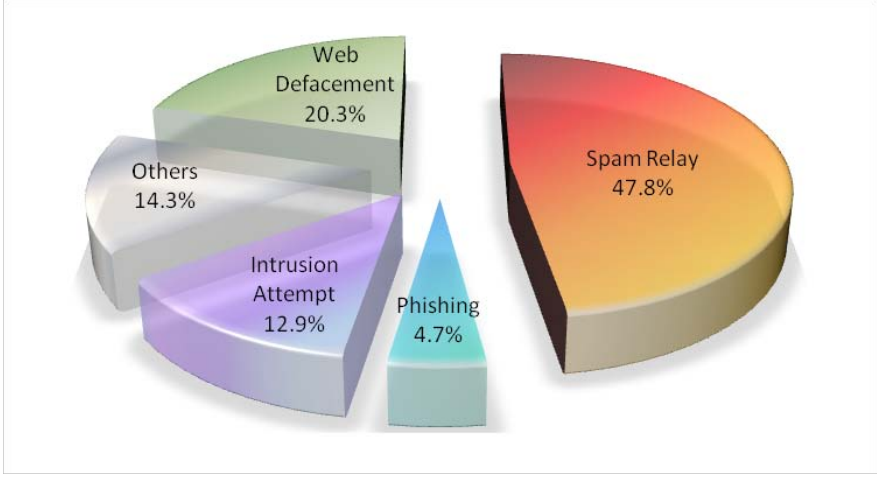
However, these figures do not necessarily imply that the damage caused by the malicious code and hacking incident is also increased or decreased. Current trend shows that the attacks are targeting more narrowed scope and specific victim rather than the anonymous majority, and the victims can be vary from individuals to corporations. Therefore, figuring out the overall damage caused by those incidents is getting more difficult, as the attacks are evolving in its aspect and methodology.

Worm/Virus

Throughout the year 2009, the number of worm/virus reported to KrCERT/CC is 10,395, which is 22.7% increase compared with that of the last year (8,469 in 2008). This is mainly due to the fact that we have seen the increase of the malware such as ONLINEGAMEHACK, which has been distributed for stealing credential information for using in certain online games and takes 10.8% of all reported malwares, followed by AGENT, which has been used for downloading additional malware and takes 10.5%, throughout the year 2009.

Hacking Incident

The total number of reports on hacking incident in year 2009 is 21,230. Among the reports on hacking incident, spam relay (10,148) takes 47.8% and has been increased 56% than that of the year 2008 (6,490).



Internet incidents reported to KrCERT/CC in 2009

The number of Phishing hosts (988) is decreased compared with that of the last year (1,163). The number of webpage defacement is 4,320 and others

3,031. The number of intrusion attempt (2,743) is decreased compared with that of the last year (3,175).

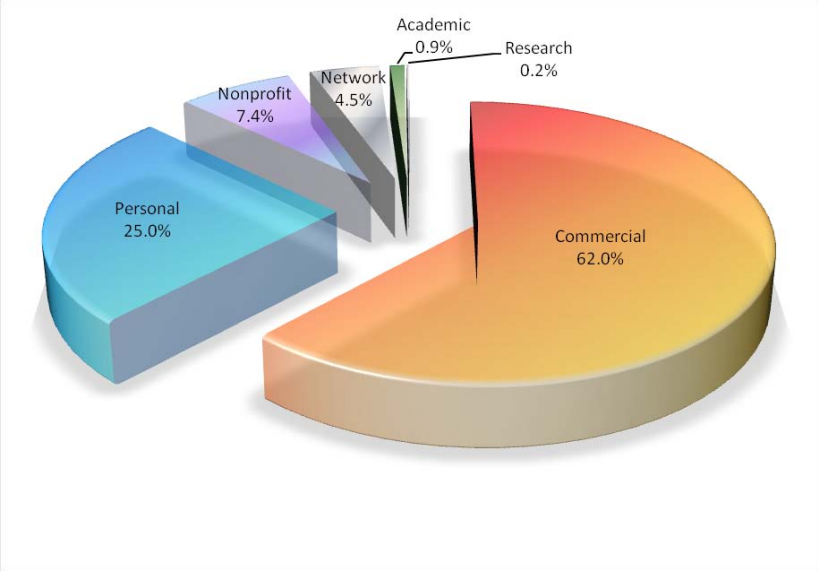
The number of Phishing and Intrusion Attempt has been decreased. On the other hand, the number of traditional incidents such as Spam Relay and Web Defacement has been increased, takes quite a portion in the entire number of incidents, taking over a half together.

Efforts to reduce malware embedded websites

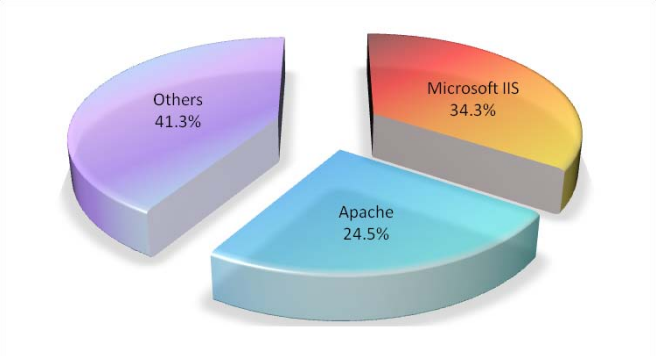
KrCERT/CC operates a malware embedded website detection and response system, so-called MCFinder (malicious code finder), which enables to detect and manage malware embedded websites. This detection system crawls and hunts for more than 180,000 websites in Korea that potentially embedded with a malware, and links to a malware in web pages. The system has a pattern database for detection to determine whether the website is embedded with a malware and/or its link, and the database is continuously updated.

Often a malware in a website inserted by a hacker spreads through Internet to users who connect to. It then penetrates to users' PCs without cognitive indication, to be abused as a Zombie or for stealing the personal data. Financial gain is often or mostly an objective for these incidents these days and this trend is rising than any moment before. This trend can be seen since many of the abused systems are eventually used as or leaded to a phishing or identity theft.

To mitigate this trend, KrCERT/CC is putting an enormous effort by monitoring and handling the malware embedded websites while taking down those sites, using the MCFinder system. The number of detected malware embedded websites in year 2009 is 7,352, which is 18% decrease compared with that (8,978) of the year 2008. We categorized them by business sectors as shown below.



Most of the web server detected in the system is Microsoft IIS web server, which takes 34.3%, Apache takes 24.5%, and others 41.3%, as shown below.

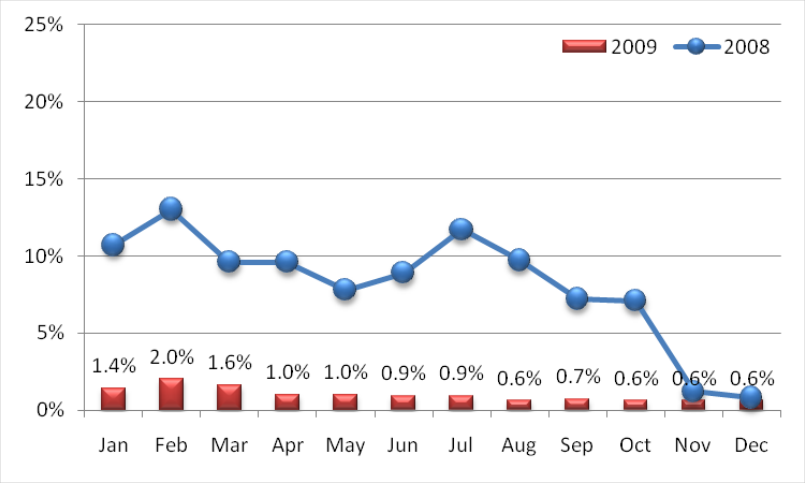


Efforts to reduce bot infection

Bot has been one of the biggest threats for recent years and detected continuously that the domestic servers are exploited as bot C&C servers. It seems that domestic servers are continuously targeted because of well-sorted infrastructure in Korea, since Bot C&C servers characteristically prefer faster network. KrCERT/CC is pouring a great effort to reduce the domestic bot infection rate, by monitoring and applying sinkhole method to the bot C&C servers, with the cooperation from ISPs in Korea.

Domestic bot infection rate has marked highest as 24.1% in January 2005, which gradually decreased month by month, and the monthly average rate of

2008 was 8.1%, which is decreased to 1.0% in 2009[2]. The graph of the domestic bot infection rate in 2009, shown below, is very steady, and average is much lower than that of the year 2008.



Monthly domestic bot infection rate in 2009

3. Events organized / co-organized

2008 APISC Security Training Course

KrCERT/CC hosted the 2009 APISC Security Training Course to support strengthening the response capabilities of the developing economies. The objective of this training course is to assist developing economies to establish Internet incident response capabilities while providing a training opportunity for establishing and managing CSIRT in their own economy. This event was held on 11-15 May in Ibis Myeong-dong Hotel, Seoul, Korea, with 21 trainees participated from 17 economies, 5 trainers from 3 economies, throughout the Asia and Pacific region.

The content of 5 days course includes general overview of the information security and Korea Information Security Agency, and TRANSITS (Training of Network Security Incident Teams Staff) course. Active participation from the trainees benefited all participants while active discussion and interaction of the trainees and trainers had been allocated for most of the time. The course was successful and fruitful as well as attendees have satisfied with the overall course.

[2] This statistics is analyzed from KrCERT/CC's honeynet system located in Seoul, Korea. KrCERT/CC is operating Bot Detection System on real-time basis.

APCERT Incident Handling Drill

Internet is in the nature of borderless and seamless network, so as Internet incident. It is characteristically not limited to one economy or region. This reality put more meaning on the importance of having an incident handling drill among many economies, cooperation between CSIRTs for various sectors. KrCERT/CC has participated in the APCERT incident handling drill in 2009 which has ended with successful result.

The drill was again to verify the coordination capabilities among CSIRTs on incident handling framework, deliver actions to improve incident response system in each CSIRT, and give participants an experience of a coordination system. 24/7 POCs were shared for preparation and an IRC channel was used for real-time communication. 16 APCERT member teams from 14 economies have joined the drill, as the scenario was not distributed before the actual drill commenced. Some economies had their own drill with local ISPs involved and played with their own coordination system with the given version of scenario. HKCERT has successfully completed to coordinate the drill, as whole other participated teams have successfully done their tasks. Yet another good drill was performed in 2009 by the APCERT members.

4. International Activities

KrCERT/CC has participated in National CSIRT meeting held in July 2009 in Kyoto, Japan, hosted by CERT Coordination Center. We learned from other CSIRTs and had a chance to build a cooperation relationship with other major CSIRTs.

In APEC TEL 40 meeting held in Cancun, Mexico, at the SPSG meeting, Mr. Jinhyun CHO from KrCERT/CC has done the task as the SPSG convenor, by leading the SPSG meeting regarding strengthening the global cyber security capability.

5. Future Plans

KrCERT/CC is planning to provide another training opportunity in the year 2010, by hosting the APISC Security Training Course, to many potential security experts as possible, by inviting them to attend our training course with

lectures and active discussions. This chance will give more skills and experience to the attendees in both legal and technical perspective, not only to ones from developing economies who plans to build a CSIRT, but also to existing teams by sharing the experience and trend from all the economies from Asia Pacific region.

Website:	http://www.krcert.or.kr/english_www
E-mail:	apcert-poc@krcert.or.kr
Phone:	+82-2-118

9. MyCERT Activity Report

Malaysian Computer Emergency Response Team - Malaysia

1. MALAYSIAN COMPUTER EMERGENCY RESPONSE TEAM (MyCERT)

1.1. Introduction

The Malaysian Computer Emergency Response Team (MyCERT) was established in 1997 to address the computer security concerns in Malaysia. With the number of computer users in Malaysia increasing rapidly each day, more vulnerable computers are exposed to threats of abuse and criminal activities. This is the essence of MyCERT's existence, providing a point of reference in resolving computer security incidents.

1.1.1 Establishment

MyCERT was established in 1997, and now operates under CyberSecurity Malaysia, a non-profit organization under the purview of the Ministry of Science, Technology and Innovation (MOSTI), Malaysia.

CyberSecurity Malaysia main roles can be summarized as follows:

- To assist MOSTI in the implementation of the National Cyber Security Policy (NCSP)
- To provide Cyber Security Emergency Services and act as the national technical coordination centre
- To conduct Cyber Threat Research & Risk Assessment
- To provide Cyber Security Quality Management Services
- To build capability in the field of cyber security (Training) and to create awareness and a culture of cyber security (Outreach)

Further information about CyberSecurity Malaysia can be viewed at: http://www.cybersecurity.my/en/

1.1.2 Workforce

As of December 2009, CyberSecurity Malaysia has about 200 staff. MyCERT has 23 staff to operate the two main services that it is providing, the Cyber999 incident handling service and Malware Research Centre.

1.1.3 Constituency

MyCERT's primary constituency is the Malaysian Internet Users. Therefore, MyCERT handles security incidents reported by Malaysian as well as foreign institutions where the sources or target of incidents are within Malaysia.

2. ACTIVITIES IN YEAR 2009

In 2009, MyCERT had received observed a growing number of targeted attacks such as defacements, intrusion, online fraud and malware leading to identity theft. In dealing with these incidents, collaboration and coordination with various parties such as law enforcement agencies, corporate IT departments and legal departments were so sought to resolve the attacks.

2.1. Incident Handling

In 2009, MyCERT handled 3564 security incidents reported to the Cyber999 service. This is a 67% increase of the number of incidents handled in 2009. In addition, the Cyber999 service also handled about 43287 incidents that occurred within CyberSecurity Malaysia's distributed honeynet network (Lebahnet). The incidents from Lebahnet are basically malware related, compromise attempts and remote file inclusion attacks.

Generally, the security incidents are categorized as intrusion, malicious code, fraud, harassment and spam. Fraud and intrusion related incidents make up about 78% of total incidents handled. The majority of the cases for fraud are phishing in nature. Incidents involving malware in particular botnet command and control, drop sites, and bot infection were also significant in year 2009.

In 2009, MyCERT issued 61 security advisories related to various vulnerabilities in applications and security events. The list of advisories can be viewed at:
http://www.mycert.org.my/en/services/advisories/mycert/2009/main/index.html

One of the major security events handled last year was Conficker (also known as Downadup and Kido). The malware exploited a relatively known vulnerability in the Microsoft Windows operating system. Other than issuing a security advisory and press release, MyCERT also worked closely with Domain Registry, the Conficker Working Group and local Internet Service Providers (ISPs) to detect and warn owners of infected computers.

Detail abuse statistics and trends are available on MyCERT's website.

2.2. Trends and Abuse Statistics

The year 2009 abuse statistics and incidents chart are as shown below:

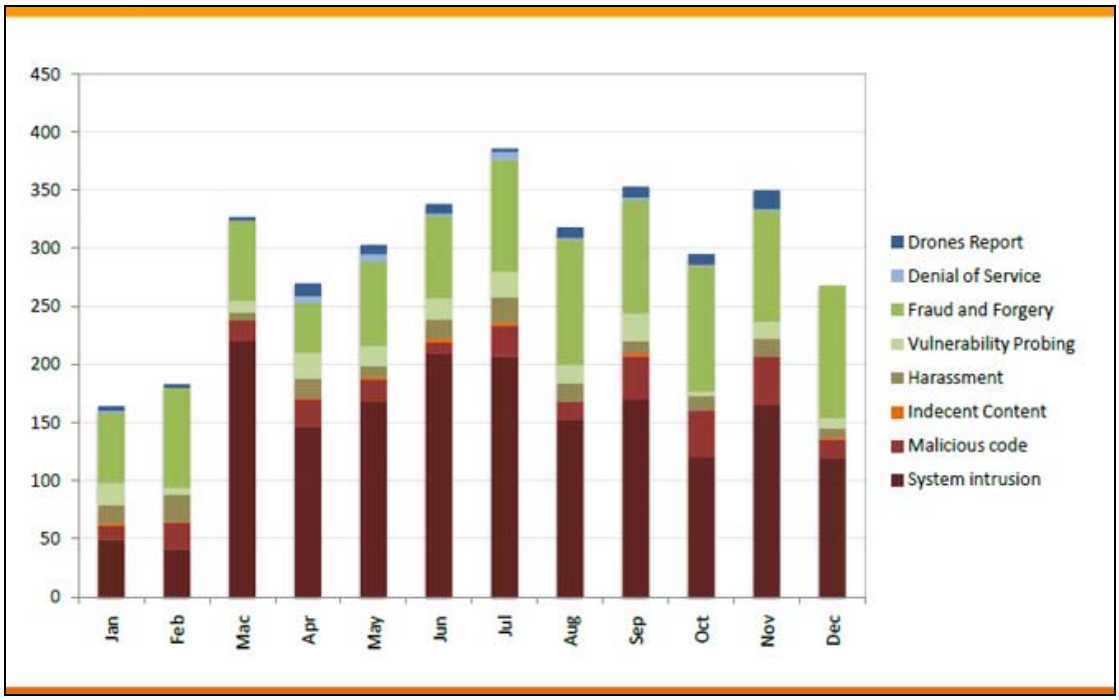


Figure 1: Incidents Handled by MyCERT in 2009

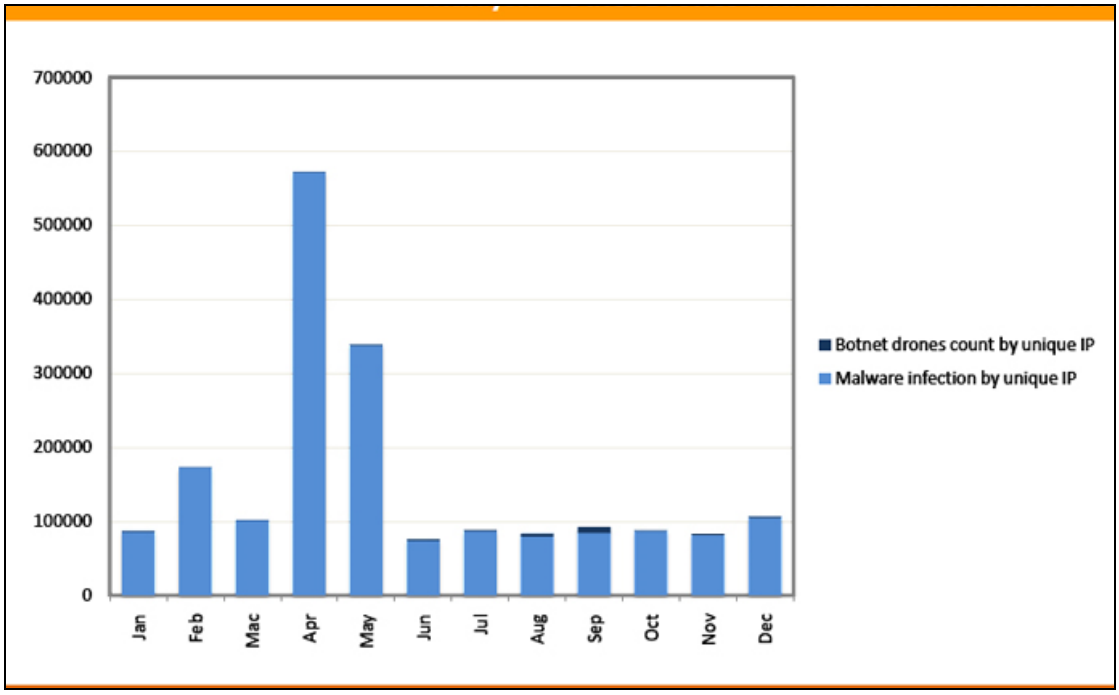


Figure 2: Infected Computers Handled by MyCERT in 2009

3. EVENTS ORGANIZED, CO-ORGANIZED AND PARTICIPATED

MyCERT had participated and organized both national and international events throughout the year. On the local scene, MyCERT had been engaged to conduct trainings and talks in the area of incident handling, malware analysis, and security trends for different kinds of audience. Internationally, MyCERT was also invited to seminars and conferences to share insights and case studies on a variety of security related topic.

3.1 Training

There were several workshops or hands-on training conducted by MyCERT in year 2009 which include:

- Hands-on Incident Handling Training, EgyptCERT, Cairo, Egypt
- Hands-on Incident Handling Training for OmanCERT, Kuala Lumpur, Malaysia
- Honeynet Hands-on Workshop at the OIC-CERT Conference 2009 (Honeynet Hands-on) , Malaysia
- Web Application Security Workshop at the FIRST Technical Colloquium KL 2009
- Web Security Training (Web Security), Malaysia

- Web Intrusion: Practical Analysis with OSS Tools at the MSC Malaysia OSS Conference 2009

3.2 Cyber Exercises

In year 2009, MyCERT had participated in two cyber-exercises:

- Annual CNII National Cyber Exercise
  MyCERT co-ordinated the cyber exercises with the National Security Council. Participants are agencies and organizations that have been gazetted as critical to the nation. The half day cyber exercise requires participants to respond to security incidents in accordance with the National Cyber Crisis Management Plan.
- ASEAN CERT Incident Drill 2009 (ACID)
  MyCERT participated as a player in the drill organized by SingCERT.

3.3 Seminars and Conferences

Cybersecurity Malaysia had organized the following conferences in 2009 that benefited security teams and players in the region:

- OIC-CERT AGM and Conference 2009
- CyberSecurity Malaysia | | Secure Asia Conference 2009
- FIRST Technical Colloquium (FIRST-TC) KL 2009

In addition to the above, Cybersecurity Malaysia organized many seminars throughout 2009.

4. ACHIEVEMENTS

4.1 Rebranding Exercise of Existing Services

In 2009, Cybersecurity Malaysia had launched officially the following services which are to be operated by MyCERT, as part of its rebranding exercise:

- Cyber999 – Incident handling and response service for the nation
- CyberSecurity Malware Research Centre

4.2 Presentations

MyCERT representative has been invited to speak at the following conferences or seminars as speaker:

- OIC-CERT Conference 2009, Malaysia
- Asia Forum of IT, Thailand
- Honeynet Project Annual Conference, Malaysia

- APCERT AGM & Conference, Taiwan
- APECTEL 39, Singapore
- Anti-phishing Working Group CECOS III, Spain
- Security Awareness Seminar - Institution of Engineering and Technology, Brunei
- FIRST Annual Conference, Japan
- ASEAN Law Enforcement Workshop – , Indonesia
- FIRST-TC (Technical Colloquium) KL 2009, Malaysia

In addition to the above, MyCERT had spoken at 60 different occasions throughout the year.

4.3 Publications

4.3.1 Alerts and Advisories

Alerts, advisories and publications such as MyCERT's quarterly report are available at MyCERT's website, http//www.mycert.org.my/

5. INTERNATIONAL COLLABORATION

5.1 Memorandum of Understanding (MoU)

As part of MyCERT initiatives to establish greater collaboration with other international teams, MyCERT, via its parent organization, CyberSecurity Malaysia, signed two MoUs that is related with CERT activities. The international organizations involved were Egypt CERT and the Taiwan Honeynet Project.

5.2 Team Sponsorship

MyCERT was one of the sponsors for Oman CERT and ECS-CSIRT (South Africa) application to become a FIRST member in 2009.

6. CONCLUSION

2009 has been another busy year in terms of incident handling and response work. It was good to learn that MyCERT's initiatives ad contribution to the nation have been recognized by important stakeholders in and outside Malaysia.

In 2010, MyCERT intends to improve the process of incident handling and embark on a couple of new projects. MyCERT is also actively seeking for

opportunities to collaborate with new partners in ensuring that the cyberspace is safe for everyone.

10. PHCERT Activity Report

Philippine Computer Emergency Response Team - Philippine

1. About PHCERT

1.1. Introduction

The Philippine Computer Emergency Response Team (PHCERT) was established to build a knowledge base of computers, internet, and other information technology related security threats and emergencies and serve as a focal point for resolving information security related incidents. PHCERT promotes information security practices by organizing regular sharing sessions as part of its awareness program.

1.2. Establishment

PHCERT was founded in 2003 as a non-stock, non-profit organization providing free assistance in the areas of policy development and security consultancy. PHCERT is a volunteer organization. Time, resources, and technical assistance are all provided "pro bono" by sponsors and members. It serves as a coordinating body between private organizations and government agencies with investigative functions with respect to reporting and filing cases involving computer related incidents.

1.3. Constituency

PHCERT's are Philippine internet users in both the public and the private sectors, including individual users. PHCERT continues to work with government agencies and technology vendors.

1.4. Membership and Workforce

PHCERT's membership and workforce consist of policy and technical researchers and information security professionals who serve on a purely voluntary basis. PHCERT's activities are coordinated through the Board of Trustees.

2. Activities

PHCERT serves as a point of contact between and among internet users in the Philippines and sometimes with organizations in other countries. As such,

incident reports are received from CERTs from within and outside of the APCERT community.

PHCERT disseminates information, including security bulletin it receives from various sources to its members.

PHCERT participates in government sponsored activities aimed at policy and rule development as well as the development and adoption of standards.

PHCERT provides assistance to investigative and law enforcement agencies in regard to information security incidents.

PHCERT provides expert advice to the judiciary, in particular, in the development of rules of court as well as creating awareness programs for the members of the judiciary.

2.1. Incident Trend

PHCERT noted an increase of incidents involving social networking activities in 2009. Many of the reports it received are from individual users who have been victimized through social engineering perpetrated by parties who assume the identity of friends and associates of the victims.

PHCERT also received reports from other CERTs involving phishing, spamming activities, information theft and fraud.

2010 is an election year in the Philippines. Related to this political activity, PHCERT received increasing reports of defaced websites of Philippine government agencies and intrusion incidents in the second semester of 2009.

2.2. Incident Resolution

The lack of a regulatory framework and policies remain PHCERT's biggest challenge. As such, incident resolution, while painstaking, is gained through volunteer members many of whom work with service providers such as telecommunications companies, internet service providers, and data centers and hosting companies. Where incident resolution prove to be difficult,

issues are sometimes referred to government investigative agencies who have the legal mandate to launch investigations.

2.3. Memorandum of Understanding

In order to improve collaborative work on the resolution of issues, a Memorandum of Understanding, which establishes a framework for reporting and feedback mechanism, is currently being negotiated with service providers such as telecommunications companies, internet service providers, and data centers and hosting companies.

3. Events

3.1. Membership and Constituency Information Sharing

PHCERT organizes regular membership meetings and constituency information sharing on information security practice.

3.2. Constituency Training

Active and encouraging support has been provided by JPCERT. As such, JPCERT and PHCERT teamed up to organize a training activity in 2009 covering subject matters as latest trends in information security, incident handling and management, overview of incident analysis, and a briefing on the Tsubame project.

3.3. JPCERT/AOTS Training

Selected members of PHCERT have been attending training programs organized by JPCERT conducted through the Association of Oversees Technical Scholarship (AOTS) for which PHCERT is grateful. The training programs cover establishment and operations of CSIRT and technical subject matters such as incident handling and malware analysis.

3.4. Seminars and Conferences

PHCERT is actively involved in locally organized seminars and conferences as a technical resource organization, providing speakers and facilitators.

4. Regional/International Collaboration

As a member of the APCERT, PHCERT serves as a point of contact in the Philippines and helps resolve internet security incidents and issues, especially those emanating from Philippine sources.

It collaborates directly with other country CERTs in resolving internet security incidents.

5. Contact Information

PHCERT may be reached at:

PHPEP Law Offices
26th Floor, Orient Square Building
F. Ortigas Jr. Avenue, Ortigas Center
Pasig City 1605, Philippines
Telephone: (632)687-5362
Fax: (632)687-4745
Email: info@phcert.org

11. SingCERT Activity Report

Singapore Computer Emergency Response Team - Singapore

1. About SingCERT

1.1 Introduction

The Singapore Computer Emergency Response Team (SingCERT) is a one-stop centre for security incident response in Singapore. Besides providing assistance to its constituency in incident resolution and co-ordination, SingCERT also broadcasts security alerts, advisories and security patches. To promote security awareness and to educate the general public, SingCERT organises frequent seminars, workshops and sharing sessions covering a wide range of security topics.

1.1.1 Establishment

SingCERT was set up in 1997 to facilitate the detection, resolution and prevention of security related incidents on the Internet. SingCERT is a government funded national initiative and is managed and driven by the Infocomm Development Authority of Singapore.

1.1.2 Constituency

SingCERT provides services primarily to the Singapore local constituency comprising of companies and end users.

2. Activities & Operations

2.1 Incident Trend

There is an increase in the total number of incidents reported to SingCERT in the year 2009 as compared to the year 2008. Phishing and the widespread of malwares were the major concerns in 2009. Besides that, there was high number of attempts and probes targeting at hosting environment and the ISPs in the early part of the year. SingCERT continues to work with other CERTs and our Internet Service Providers (ISPs) to track down affected users and keep them informed on how to secure their systems. On the regional and international fronts, collaboration and cooperation among CERTs have proved effective in the resolution of many of our cross-border incidents.

3. Events organised / co-organised

3.1 Seminars and Workshops

In our continued efforts to keep our constituency updated on security trends and developments, SingCERT organised 4 seminars for the year 2009. These events were co-organised with industry partners to bring the latest technology and knowledge to our security practitioners. The department also organizes a yearly seminar for the public sector featuring renowned speakers from overseas.

3.2 ASEAN CERTs Incident Drill 2009

The ASEAN CERTs Incident Drill was conducted on 23 July 2009. 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.

4. Future Plans and Projects

SingCERT, will be organising the 5th ASEAN CERTs Incident Drill for the year 2010. Discussions are in progress to work out the scope and coverage.

12. SLCERT Activity Report

Sri Lanka Computer Emergency Response Team - Sri Lanka

1. About SLCERT

1.1. Introduction

The Sri Lanka Computer Emergency Response Team (SLCERT) is the Center for cyber security in Sri Lanka, mandated to protect the nation's information infrastructure and to coordinate protective measures against, and responses to cyber security threats and vulnerabilities.

1.1.1 Establishment

As the national CERT of Sri Lanka, SLCERT acts as the focal point for Cyber security for the nation. It is the single trusted source of advice about the latest threats and vulnerabilities affecting computer systems and networks, and a source of expertise to assist the nation and member organizations, in responding to and recovering from Cyber attacks.

In anticipation of increased cyber security incidents as Sri Lanka's IT infrastructure grows, SLCERT was established on 1st July 2006 as Sri Lanka's National CERT, by the ICT Agency of Sri Lanka (ICTA). ICTA is the Government Agency for the development of IT Infrastructure and Policy in Sri Lanka. SLCERT is registered as a Private Limited Liability Company, and is a fully owned subsidiary of the ICTA, which in turn is fully owned by the Government of Sri Lanka.

1.1.2 Workforce power

SLCERT currently has a total of seven security team members including a Manager Operations and a COO. The staff are highly skilled and have been trained on various IT security certifications, such as GCIH, MCSE, CEH, CCNA, CCSP and CISSP.

1.1.3 Constituency

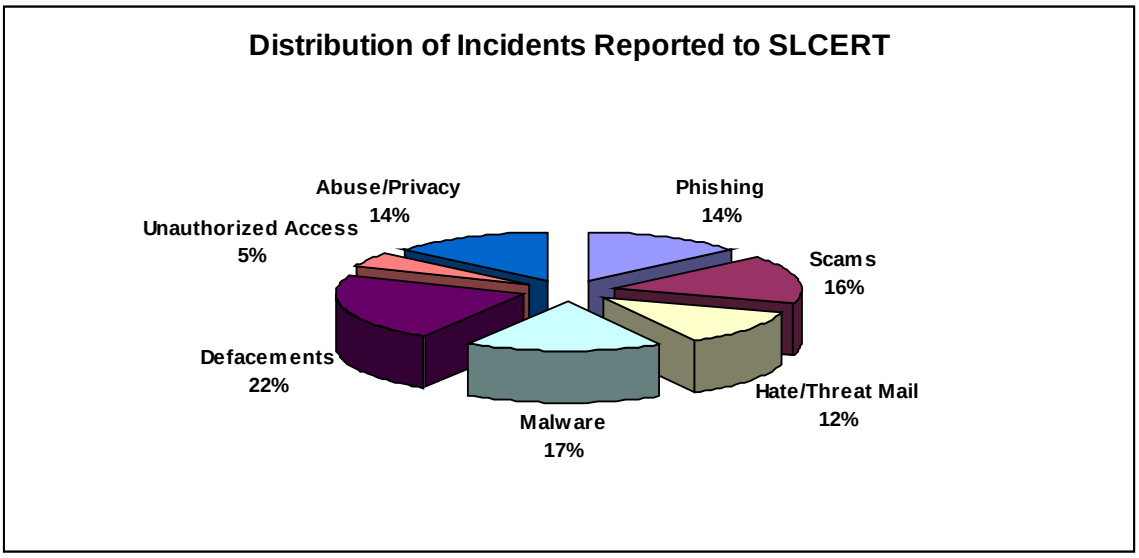
SLCERT's Constituency encompasses the whole of the cyber community of Sri Lanka (Private & Public sector organizations, and the general public).

SLCERT maintains a good rapport with government and private establishments, and extends assistance to the general public.

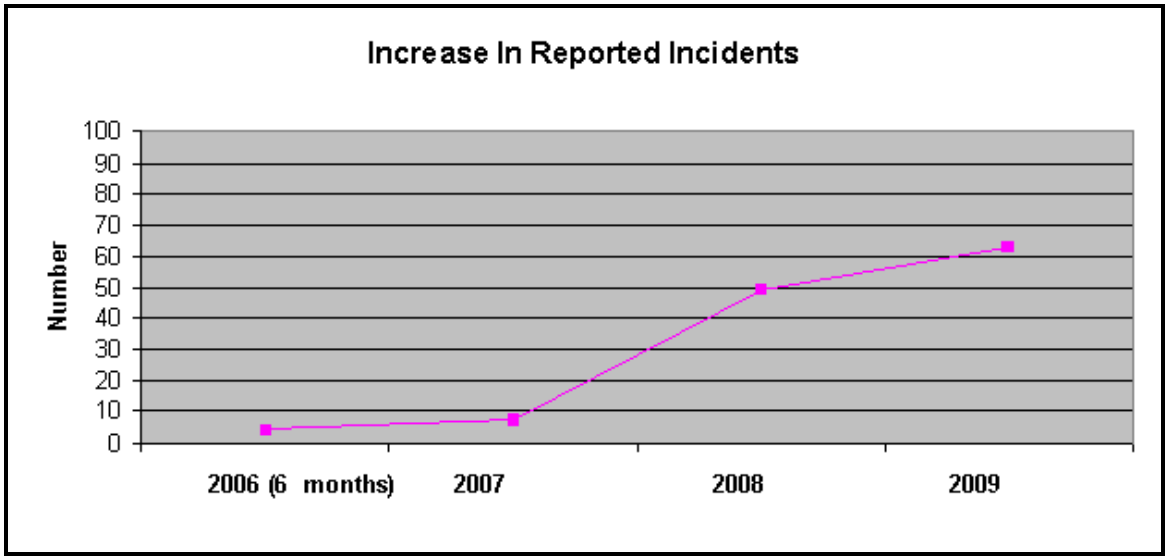
2 Activities & Operations

2.1 Incident Handling Statistics

Incidents reported to SLCERT increased up to 69 in the year 2009. This is a major hike in the number of incidents reported compared to the 49 incidences reported in 2008. The following chart depicts the distribution of various types of incidents reported to SLCERT. All the incidents reported to SLCERT have been resolved satisfactorily.

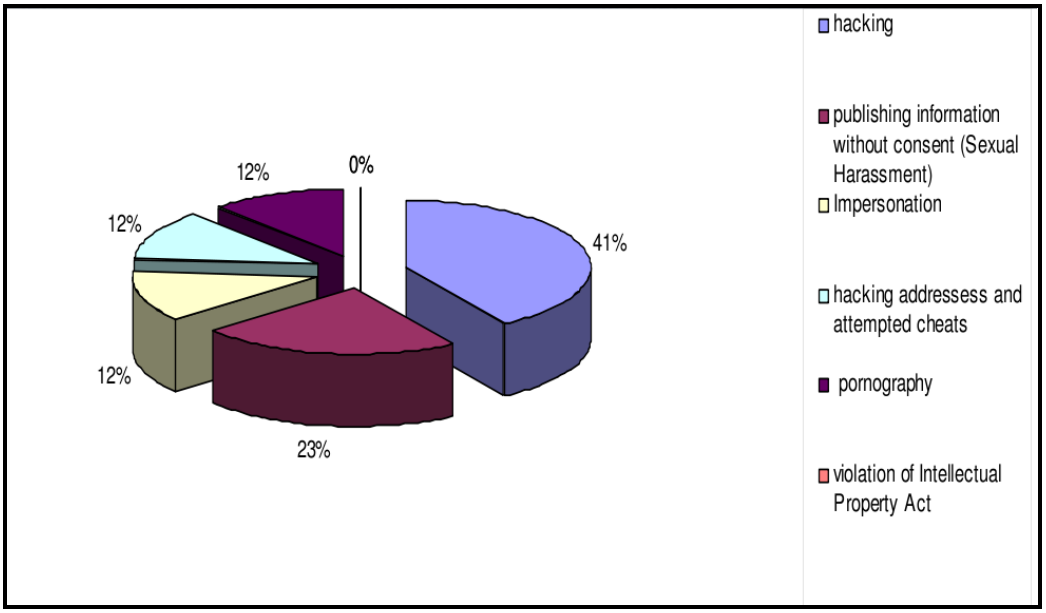


The following graph depicts the increase in the number of incidents since the inception of SLCERT in mid-2006.



2.2 Computer Crime Statistics

Sri Lankan Government introduced a new act titled Computer Crimes Act in 2007 to curb electronic crimes in Sri Lanka. The following graph depicts the number of computer crime related offences reported to Sri Lankan law enforcement agencies in year 2009.



2.3 New services

2.3.1 Behavioral Analysis of Malware

SLCERT started work on behavioral analysis of malware in the first quarter of year 2008 in order to provide better recovery procedures for affected constituents. In the year 2009 SLCERT received a number of malware samples from government institutions for analysis. SLCERT has now acquired lab equipment to analyses malware in standard environments.

2.3.2 Digital Forensics

The Computer Crimes Act of 2007 enabled the law enforcement officers to obtain the technical expertise of recognized information security professionals and organizations to extract and present digital evidence in court. Accordingly, SLCERT has assisted Sri Lankan law enforcement agencies in carrying out forensic investigations.

2.3.3 Penetration Testing

There were some major attacks on critical information systems in Sri Lanka during 2008. As a proactive measure SLCERT has been assigned the task of carrying out vulnerability assessments and penetration tests for some major information systems. SLCERT started this service during the fourth quarter of 2008.

3 Events organized / co-organized

3.1 Training / Education

SLCERT organizes training programs and education sessions targeting various audiences including CIOs, Engineers, System Administrators, Banking and telecom sector staff, Students, and general public.

During the year 2009 SLCERT conducted the following training, education programs successfully:

1. Lecture on "Information Security" for MBA students
2. Conference on Information Security for CIO's of Government Departments
3. Participated in a number of IT exhibitions by taking stalls with a view to educating the general public on IT Security

3.2 Consultancy

SLCERT provides consultancy services for requests, especially for government departments.

During the year 2009, the following consultancy services were provided:

1. Network reviews for 6 government departments
2. Forensics investigation support for Law enforcement
3. Setting up a CA server for a government department
4. Initiated the implementation of a new computer forensics laboratory for Police Department

3.3 Seminars & Workshops

Cyber Security Week 2009

Cyber Security Week 2009 is an annual event being organized by SLCERT since the year 2008, held in the month of August, which featured a series of events:

- Two Workshops for professionals, namely:

- Web Application Security (two day workshop)
- Malware Analysis (two day workshop)

➢ Two-day Conference

4 Achievements

4.1 Presentations

1. Conducted 3 lectures related to IS for Chief Information Officers (CIO) of government organizations following MBA in e-Governance.
2. Conducted Presentations on following topics during the Cyber Security Week 2009 (CSW_2009) Conference in August 2009:
   - Malware analysis-Case study
   - DDoS attack developments
   - Digital Forensics practices
   - Managed security services
3. Economy update for Sri Lanka at the SAARC Cyber Security Workshop New Delhi, India.

4.2 Publications & Other media

1. Web site
   Through the SLCERT website published security related awareness details for the public via News, Alerts and Knowledge Base. Glossaries, case studies, FAQs are among some of the published items.
2. E-mails
   Disseminating security related information via e-mail alerts to SLCERT Website susbscribers.
3. Newspapers / media
   Educated the general public about SLCERT's role in combating cyber crimes through the electronic media.

4.3 Certification & Membership

4.3.1 Security Certifications obtained by staff members within the period:

CEH (Certified Ethical Hacker) from EC Council was obtained by four staff members of SLCERT

4.3.2 Memberships obtained in professional security organizations in the period 2008:

APCERT Full Membership

5 International Collaboration

5.1 MOU

MoU between SLCERT & JPCERT/CC (Japan) on 1st July 2009 to serve as a partner in the Tsubame Network Monitoring System for the Asian Region.

5.2 Mentor(s)

JPCERT/CC

5.3 Event participation

1. March 4th -5th
   APCERT AGM
   Taiwan
   In view of its active participation, SLCERT has been encouraged to join the Steering Committee of the APCERT and also to join two working groups.
2. May 11th - 15th
   APISC Training
   Seoul, South Korea
   Presented a paper on economy status, CSIRT establishment and incident handling procedures.
3. June 28th – July 2nd
   21st Annual FIRST Conference
   Kyoto, Japan
   Voted at AGM, attended APCERT Steering Committee meeting, new contacts made.
4. December 15th
   ISACA Annual Conference
   Colombo, Sri Lanka
   Gained practical knowledge on Audit methodologies, made new local contacts, did a presentation on Practical Digital Forensics.
5. December 22nd - 23rd
   Attended a SAARC Workshop on “Cyber Security”
   In New Delhi, India

Able to get an understanding on the issues of Cyber security in the SAARC region and had good networking opportunities with member countries.

5.4 International incident coordination

Details on incidents suppressed to prevent unauthorized disclosure. Dealt with the following entities to mitigate cyber security incidents.

1. MyCERT
2. Internet Identity
3. BrCERT
4. CERT/CC
5. Virginia Tech
6. CERT Hungary

6 Future Plans

6.1 Future projects

The following projects are either in the conceptual stage or just been initiated, and are intended to serve the constituency directly:

1. Certificate Authority server for Nationwide Government Network
2. Setting up sectoral CSIRTs and organizational CSIRTs in the economy
3. Additional Sensor deployment for "Tsubame" project, to cover 32 IP Address ranges belonging to Sri Lanka

6.2 Framework

6.2.1 Future Operations

This section details the changes anticipated in SLCERT with regard to staff, equipment and capabilities:

Retaining trained staff has been a constant challenge for SLCERT. Staff turnover is not high, but SLCERT lost a very senior hand during the course of the year. New staff is competent, but the real challenge is the cost of get proper training for this new staff.

6.2.2 Operations Support projects

These have been initiated to develop internally or procure necessary applications, hardware and personnel to support SLCERT's core business functions:

Setting up a fully equipped digital forensics laboratory for SLCERT will be top priority in the year to come.

7 Conclusion

Being nearly four years old, SLCERT has faced an uphill task of raising awareness of Information Security in Sri Lanka. The increase in the number of incidents reported and handled by SLCERT in consecutive years is a testament to the success of SCERT's awareness campaigns.

SLCERT shall now focus on extending its service offering, while streamlining existing services so as to achieve maximum effectiveness with its staff strength. Focus shall be redirected on training staff in the necessary competencies to ensure continued operation.

SLCERT shall continue to participate in regional events such as the Annual APCERT drill and also welcomes opportunities to collaborate with its sister CERTs in incident coordination.

Year 2009 was named as the year of ICT and English by the government of Sri Lanka, that gave SLCERT a further impetus. With this in mind SLCERT will continue to conduct the annual Cyber Security Week conference and workshops while finding new ways to reach an even wider audience.

We look forward to being a bigger part of APCERT in 2010 by contributing to various working groups and activities to build a safe and secure cyber space for the world.

13. TWCERT/CC Activity Report

Taiwan Computer Emergency Response Team/Coordination Center - Chinese Taipei

1. About TWCERT/CC

Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) is a security organization for computer intrusion handling, security-related resource and tools providing, latest vulnerability information publishing, and security education popularizing. In addition to play a coordination role in domestic security domain, TWCERT/CC actively participates in international network security organizations and actions to strengthen communication and coordination with CERTs. Expect to provide users with a safe and convenient internet environment under cooperating with domestic and international security organizations.

TWCERT/CC formally established since 1998. The major purposes of TWCERT/CC are to prevent and actively assist the computer and network security incidents in Taiwan, to analyze the system vulnerabilities, to provide computer and network security tools and related documents for the system administrators and the programming guidelines for the developers, and conduct a series of training programs to raise the awareness of network security. TWCERT/CC is constantly reinforcing the organization functions and refining the network security services. With the dedicated devotion and seamless collaboration of the whole team, TWCERT/CC has accomplished several significant gradational goals and missions as follows:

(1). To assist the handling of the intrusion incidents around the region.
(2). To announce the system vulnerability information.
(3). To provide security training and education on protection and defending technologies and skills.
(4). To research and develop the Security Auditing System (SAS) which audits the subscribed client systems.
(5). To assess periodically the regional security level in the Internet.
(6). To be the official international coordination in Taiwan by joining international security organizations.

The main purpose of TWCERT/CC is to provide assistance to handle the incidents regarding information and network security. By raising the attention of network community to security issues and conducting the research on computer systems, we manage to enhance the fail-safe systems of computers and networks, and proceed to prevent the incident before hand. Following are our chief missions:

- Speed up the circulation of network security information to enhance the safety of domestic information and networks.
- Research and develop the computer network detecting and defending skills to strengthen the network safety.
- Facilitate the foundation of each organization's emergency response team, promote the regional network security, and reconcile the combination and interchange on security information.
- Encourage and coordinate the exchanges and cooperation between each international emergency response institution to maintain the global network security.

2. Activities & Operations

■ Domestic and international security incidents advising and handling

Frequent incidents show that it is great urgent to improve system and network security. To defend hacker intrusion and stop up security threats spreading, TWCERT/CC works hard for safeguarding security and plays the contact agent for sharing the experiences on dealing Taiwan's network security incidents with other CERTs. Expect to achieve the following goals:

(1) Possible incidents prevention: provide an incident response channel and the prevent mechanism for the victims to avoid analogous events happening.
(2) Real-time Incidents handling: offer an immediate warning and defense force to effectively restrain and control incidents extending.
(3) Recovery support: provide technological consultant and support to recovery operation and reduce damage.

Year	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008
Total	9	85	962	1260	5318	2874	1824	788	660	1087

Table 1. TWCERT/CC incident response statistics

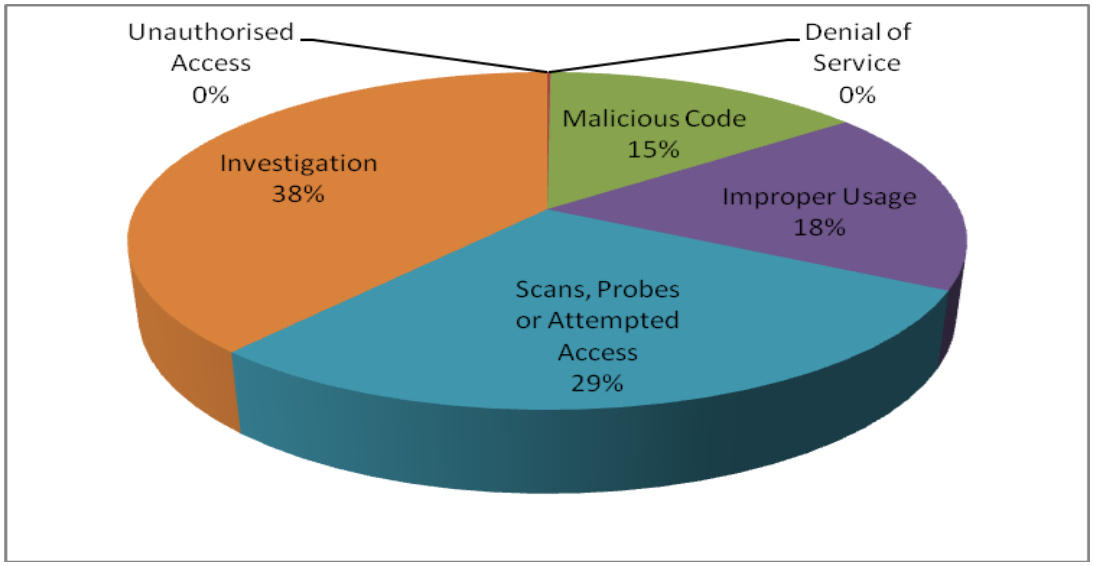


Figure 1. TWCERT/CC incident response classification statistics

- **Security Vulnerability Announcements**

To promote system and network security and reduce damage from intrusion, TWCERT/CC is devoted to strengthen services, to publish latest security issues, to provide security documents/tools, vulnerability patch information and security related documents download, and actively research attack/defense technologies.

Year	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008
Advisory	186	178	172	258	142	197	140	138	119	49

Table2. TWCERT/CC advisory statistics

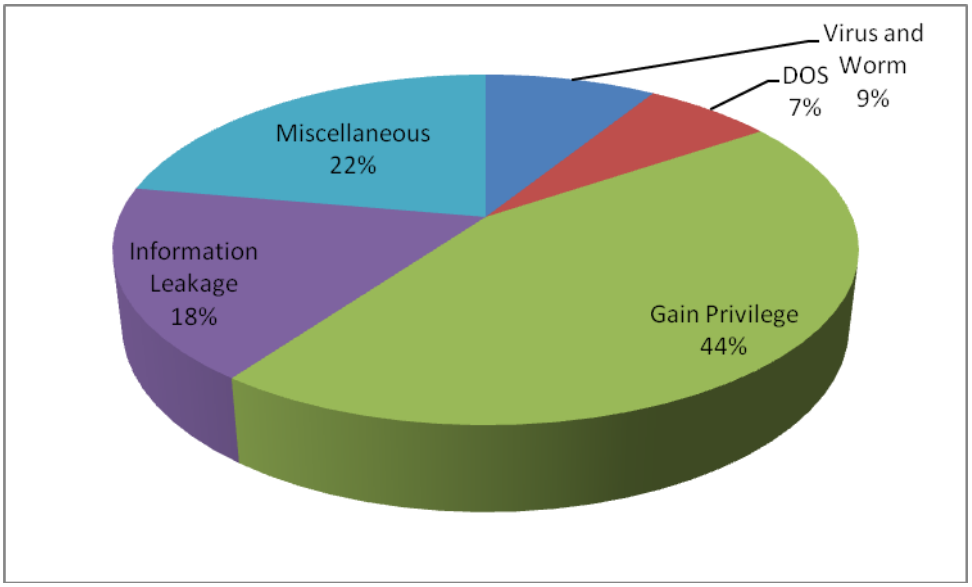


Figure 2. TWCERT/CC Advisory Classification

- **Mailing list subscription**

TWCERT/CC has collected and compiled security documentations and the advisories from various foreign hardware and software companies. The information has been evaluated and translated into the localized language, the staff dispatches to the Taiwan publicity to achieve the synchronicity of worldwide circulating information as soon as possible. In addition, the monthly TWCERT/CC Newsletters include special columns on the latest network security information, technologies, or skills to raise the awareness of network security in Taiwan.

- **Information Security News Update**

TWCERT/CC researches, analyzes and develops technology and training aimed at helping administrators to secure their systems and networks. TWCERT/CC irregularly provides security related information, such as security tools, advisory, vulnerability remediation, technology documents, for the multitude and security-conscious users to enhance security education and consciousness.

- **Remote Security Auditing System maintain**

Systems or applications bugs and vulnerabilities are exploited to cause most incident events and unauthorized access. TWCERT/CC established an on-line

Security Auditing System to provide customers self-check system vulnerabilities and patch without downloading/ installing/upgrading any software. Security Auditing System is a fortification of risk management tools, which is as important as firewall, anti-virus software and IDS. Security auditing system helps administrators understand the potential vulnerabilities and threats of their administrative domain. By continuing research and development, TWCERT/CC Security Auditing System will provide better and convenient service to accomplish the following design goals:

A. Convenience
   - User-friendly interface and easy-to-use
   - Flexible configuration and setup

B. Reliability
   - Reliable and efficient scan

C. Integrity
   - Graphical statistical report
   - Suggested and related advisories in the report

■ **Chinese Vulnerability Database maintenance**

The major purpose of the establishment of the Chinese Vulnerability Database is to collect the information of software vulnerabilities and system weaknesses. The vulnerability database contains 49 categories and up to 29 thousands records. We will continuously invest manpower to maintain and update. The major categories are shown in Fig. 3.

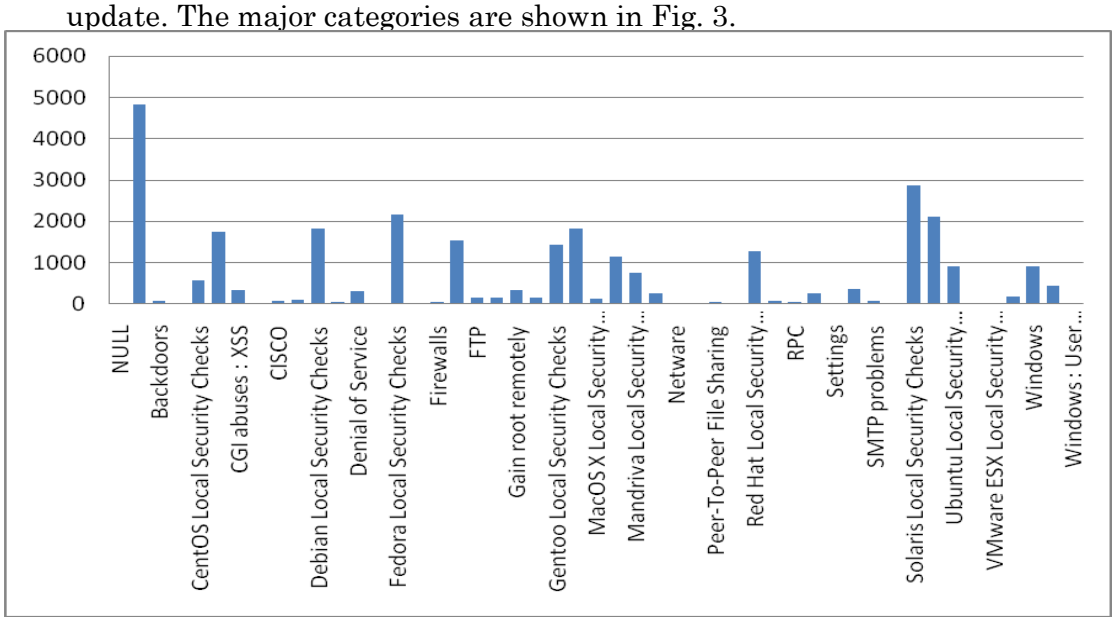


Figure 3. Categories of TWCERT/CC Vulnerability Database

- **Information Security Training**

TWCERT/CC provides a series of security training/education for government agencies and industries to enhance and enrich their knowledge and capability on network and information security. The training course also gives people a channel to exchange information and hands-on practice related to security. By adopting e-learning, TWCERT/CC education courses feature a synchronous/asynchronous on-line learning, a flexible study schedule, and independence learning without time/space restriction to accommodation the different needs of the learners.

- **Spam analysis report**

TWCERT/CC statistics and analysis spam on a regular basis. With regard to this spam statistics, totally analyzing 776,736 spam dates from January 14 in 2008 to September 17 in 2009.There are more detail information in 301,026 spam, with this analysis. Most of the results aimed at 301,026 spam. The 301026 spam come from 6624 IP addresses, send to 12492 IP addresses. Average 45 spam is from the same source IP, (The sender IP is probably fake.) and target IP averagely received about 24 spam.

Data collection start	2008-01-14
Data collection end	2009-09-17
Total emails collected	776736(301026)
Unique source IP addresses	6624
Unique target IP addresses	12492
Unique ISP sending spam	5

Figure 4. General statistics

Sources of the spam are five Taiwan's ISP industry, including HiNet, TFN, Seednet, APOL and So-net. Figure 5. Shows HiNet sent the highest proportion

of spam, second is TFN, about 20 per cent, following is Seednet, APOL and So-net.

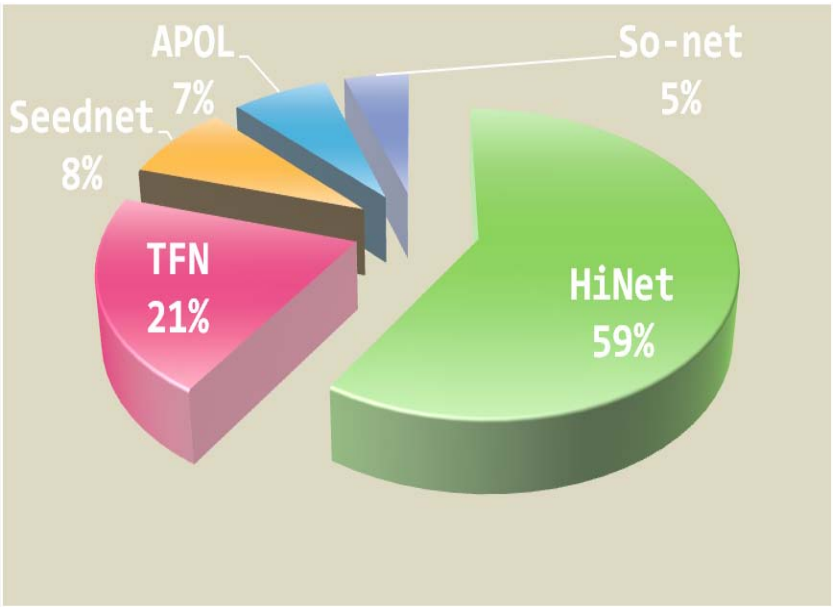


Figure 5. ISP of the spam sources

Figure 6. shows the location of target IP, about three quarters spam sent to Taiwan. Quarters are USA, UK, CN, N/A and other.

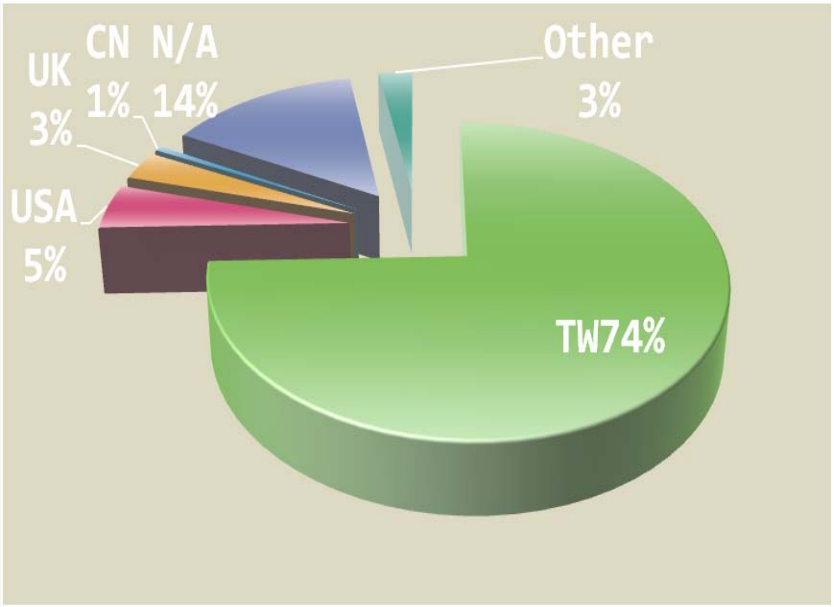


Figure6. show the location country of target IP.

Figure 7 show the statistics of e-mail address domain of spam receiver and spam amount percentage of each e-mail domain received. We can see the most spam receiver is HiNet

email domain. Second is Yahoo, with 25 percent. Others likes Gmail, Hotmail, Seednet, and Pchome obvious less than HiNet and Yahoo.

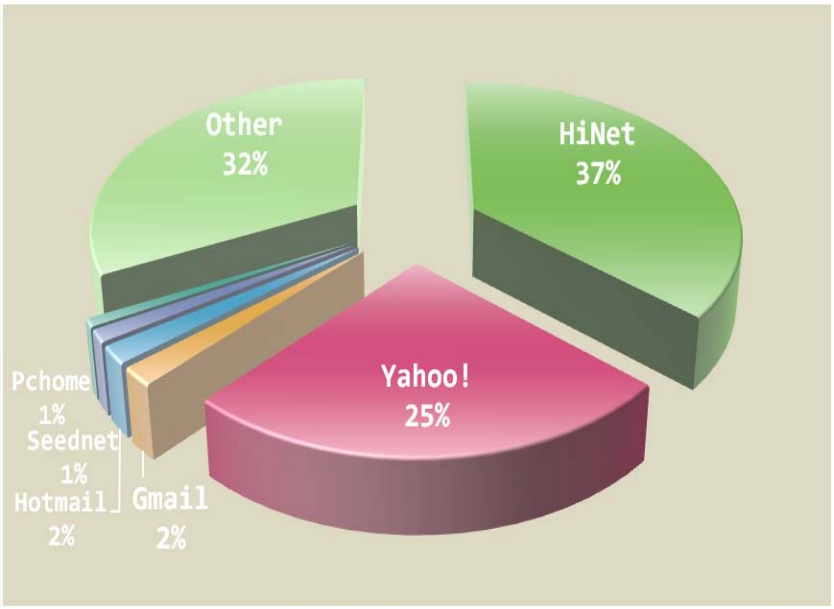


Figure 7. show spam amount percentage of each e-mail domain received.

In general, spammers in order to hid the sender's source IP, they use Open Proxy or Open Relay to delivery spam. Figure 8.shows the per cent of port 25, port 1080 and other port use situation. About 85 percent use Open Proxy, 14 percent use Open Relay.

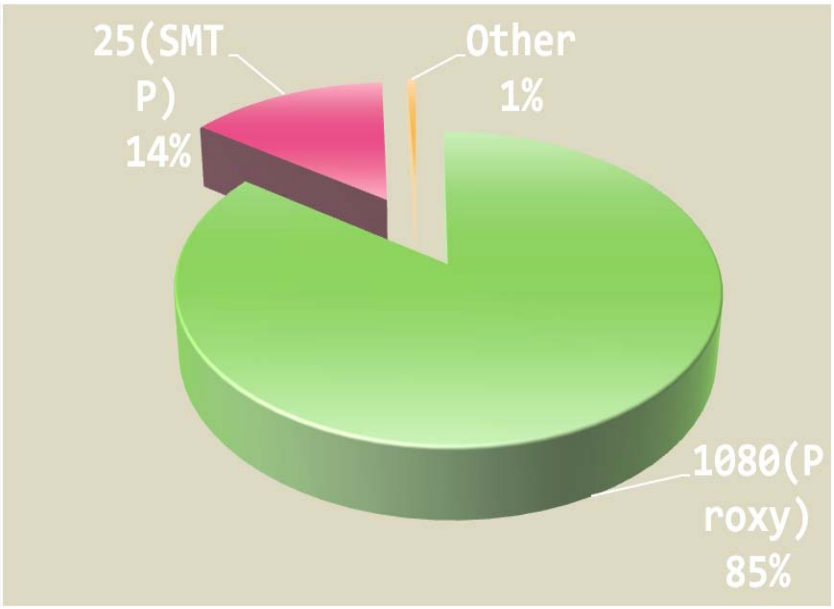


Figure 8.shows the per cent of port 25, port 1080 and other port spammers use for delivery spam.

■ Member Services

TWCERT/CC offers products, service and resources to help registered members find the best approach to security and continuously researching various aspects of computer security to benefit our members.

3. Events organized / co-organized

3.1. Information Security Training

TWCERT/CC hosts seminars or training regularly to popularize network security knowledge, to enhance system administrators' skills, and provides a good interaction channel for personal training and education promotion.

Date	Subject
2009/12/18	Malicious E-mail Social Engineering Training
2009/11/04	Anti-Spam Training
2009/10/02	Information Security Management System and Risk Assessment
2009/09/11	The analysis of Malicious code and Digital Forensic
2009/08/19	Personal Data Protection
2009/08/13	Unix-like System Security
2009/08/12	Introduction of Information Security Auditing System
2009/07/16	Information Security Promotion
2009/05/05	Anti-Social Engineering Training

Table 3. Timetable of TWCERT/CC Training

3.2. Seminars

Date	Seminar	Host	Location
2008/11/24 | 2008/11/25	Taiwan-Germany Information Technology Workshop 2008	TWISC	Kaohsiung, Taiwan
2008/07/07 | 2008/07/77	Security Camp 2008	TWISC	Tai-Nan, Taiwan
2008/03/10 | 2008/03/12	2008 APCERT Annual Meeting	HKCERT	Hong Kong, China

2008/04/16 | 2008/04/18	Info Security 2008	Isecutech	Taipei, Taiwan

Table 4. Timetable of Seminar

4. Achievements

4.1. Services

The government and organizations recently pay much attention to information and communication security promotion and development. TWCERT/CC has made great efforts to manage in security field many years for enhancing network safeguard to protect against the increasing intrusion and attack.

- **Enhance domestic network security**

  The main purpose of TWCERT/CC is to provide assistance to handle the incidents regarding information and network security. By raising the attention of network community to security issues and conducting the research on computer systems, we manage to enhance the fail-safe systems of computers and networks, and proceed to prevent the incident before hand. We disseminate system vulnerability information to raise the awareness of network security, identify and resolve the system vulnerabilities on various platforms, and work with security researchers to develop the prevention and protection techniques to improve the network security.

- **Encourage and coordinate incident response**

  TWCERT/CC is devoted to promote collaborative research and development on cyber security to reduce the loss caused from incidents. TWCERT/CC plays a major communication agent for encourage and coordinating the exchanges and cooperation with domestic ISPs and international CERTs or CSIRTs to maintain global network security.

- **Security training/education promotion**

  TWCERT/CC works to create an international workforce skilled in information assurance and survivability by developing curricula and training for executives, managers, engineers, network administrators and

operators. Furthermore, TWCERT/CC hold seminars and education training programs to publicize the network security information and to enhance the capability of the security administrators in a more active way. Such interactively training provides a great channel for information sharing as well as skill improvement.

- **Personnel training**

  Recently frequent incidents encourage security awareness and professional demand. Personal training is the major work in technology development. TWCERT/CC offers many introductory and advanced training for executive, managers, educators, engineers, cyber administrators/operators and so on. TWCERT/CC has trained many good talent of security field who are responsible for the security of information assets in different organizations. Hope to enhance domestic research and development capacity by mutual support and cooperation.

- **International communication**

  TWCERT/CC actively participates in international organizations and activities, and improves our capabilities and services. We have joined in FIRST, APCERT and Anti-spam MoU to be the international coordination in Taiwan to reinforce the information exchange and collaborations among all the other CERTs around the world. On account of the cooperation among the network security organizations, we expect to provide a secure and convenient network environment for the Internet users.

4.2. Certification

- ISO 27001 Lead Auditor
- ISO 20000 Lead Auditor
- Certified Ethical Hacker

5. International Collaboration

In addition to make efforts in security improvement in our domain, TWCERT/CC actively participates in the international security organizations and actions to enhance communication and cooperation. TWCERT/CC played a major communication agent for encouraging and coordinating the exchanges

and cooperation with the international emergency response institutions to maintain the global network security.

- To participate in international forums and meetings, to exchange the related security intelligence with each emergency response center.
- To form a transnational defense system to handle international incidents.

- **Forum of Incident Response and Security Teams (FIRST)**

FIRST is the Forum of Incident Response and Security Teams. It was clear from then on that information exchange and cooperation on issues of mutual interest like new vulnerabilities or wide ranging attacks - especially on core system like the DNS servers or the Internet as a critical infrastructure itself - were the key issues for security and incident response teams. FIRST brings together a wide variety of security and incident response teams including especially product security teams from the government, commercial, and academic sectors.

TWCERT/CC becomes the first official international coordination in Taiwan by joining the FIRST in October 2001 to share the latest security information and technologies in FIRST forum with members, attends annual FIRT conference to establish a transnational security joint defense system and enhances incident-handling capability for integrated early-warning mechanism.

- **Asia Pacific Computer Emergency Response Team (APCERT)**

Besides globalization organizations, Asia Pacific Computer Emergency Response Team is a regional coordination organization established by countries of the Asia Pacific region in 2002 to enhance regional and international cooperation on cyber security. APCERT cooperates with CERTs and CSIRTs to maintain a trusted contact network of security experts in the Asia Pacific region to improve the region's awareness and competency in relation to cyber security incidents.

TWCERT/CC jointly develops measures to deal with large-scale security incidents and phishing attack, and exchange technologies and experiences with APCERT members to manifest Taiwan much effort in security and help to understand the latest development and tendency in the Asia Pacific region.

- **Seoul-Melbourne Multilateral Memorandum of Understanding on Cooperation in Counting SPAM**

  E-mail becomes a major application with the population of computer and network, however, the following spam abuse is getting more and more rampant. Spam not only wastes individual and enterprise cost, but also endangers information and network security. Enterprises and the government have to face and restrain the spam threat which is a global authorized problem. In addition to legislation and management, the most important is to set up a transnational and trans-organizational cooperation to effectively stop spam persecution.

  Seoul-Melbourne Multilateral Memorandum of Understanding on Cooperation in Counting SPAM is an agreement signed by Australian Communications and Media Authority (ACMA) and Korea Information Security Agency (KISA) in 2003. Participates in Seoul-Melbourne MoU are part of a network of computer security incident response and security teams that work together voluntarily to deal with spam problem and prevention.

  TWCERT/CC has been promoting the training of computer-network security response for years. Since 2005, TWCERT/CC has officially joined Seoul-Melbourne MoU member, and played the contact agent for sharing the experiences on dealing Taiwan's spam issues and exchange the anti-spam jurisdiction process with other members.

  The key points of our missions are:

  - To cope Taiwan's network security incidents with other nations, and take the part as a coordination center;
  - To assist in handling the transnational spam problems;
  - To exchange the related security intelligence with each member;
  - To participate in international forums and meetings related to network security, and to uplift Taiwan's international image and position.

6. Future work and Conclusion

I order to keep the international influence, to participate in transnational operation and to ensure the basic right of the Internet users, TWCERT/CC wishes to enhance the international competitive ability and visibility of Taiwan

and practice in international communication by promoting security sense and transaction.

- Work for security related research and development to advance the international visibility.
- Participate in international interchange and coordination to form a transnational joint defense mechanism.
- Jointly developing measures to world-scale network security incidents and know well the international security tendency and development to advance global internet environment.
- Train the awareness and capability in information security and risk management through information sharing and international cooperation.

14. TWNCERT Activity Report

Taiwan National Computer Emergency Response Team - Chinese Taipei

1. About TWNCERT

TWNCERT domestically as known as ICST (Information & Communication Security Technology Center) is the leading CSIRT in Taiwan public sector. TWNCERT is intended for improving incident response and information security awareness in Taiwan. It is mainly dedicated to create a response center that can help optimize the capability of real-time monitoring, coordination, response and handing in the face of security incidents.

The missions of TWNCERT include:

- To coordinate among relevant agencies and organizations to identify pertinent response and actions in case of security incident.
- Providing an information exchange center for information at home and abroad.
- To help relevant government agencies to set up computer emergency response team (CERT).
- To provide government agencies reference information for formulation of security policies.

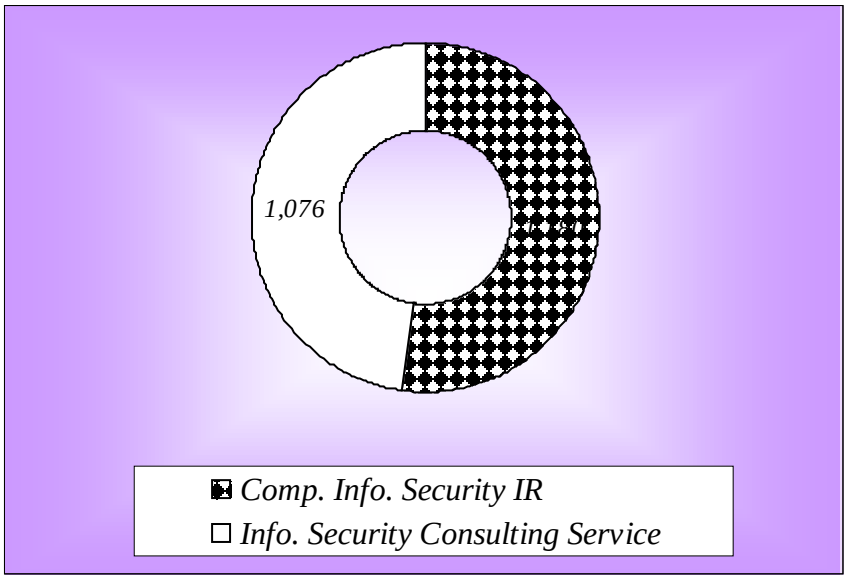
TWNCERT services including:

- Alert and publication: Guarding against and publishing probable security threats (e.g. vulnerability analysis).
- Technical service: Providing technical service to government agencies.
- Assistance in the setup of CERT: Assisting interested agencies to set up their own CERT.
- Consultation: Making suggestions regarding operation and R&D of computer security and Internet issues.
- Strategy recommendation: Making suggestion to government agencies regarding strategic planning.
- Risk analysis: Undertaking risk assessment.
- Collaboration: Building collaborative relationship with legal community, information security business and ISP.

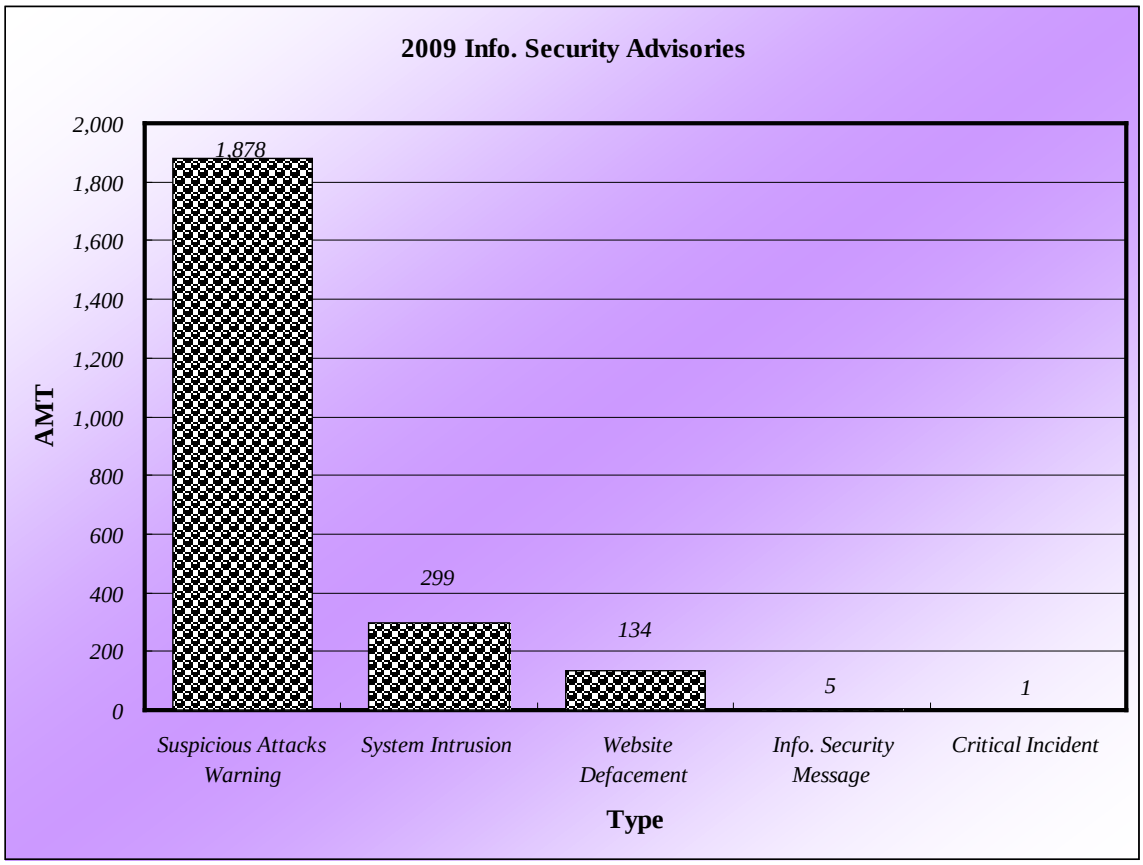
- Coordination: Building coordination and communication channels with domestic and foreign incident response organizations.

2. Operations & Activities

- In 2009, TWNCERT received 1,180 reports on computer information security incidents from Taiwan government and academic sectors。 TWNCERT also offers 1,076 information security consulting service and 16 serious governmental information security incident handling.



- TWNCERT cooperated with Taiwan Academic Network (TANet) and collected totally 5,256 malware samples. Moreover, TWNCERT traced down the Botnet activities and published 12 C&C advisories and 121 Botnet activities warning advisories. Also TWNCERT infomed JPCERT/CC and KrCERT/CC of 11,243 attack source IPs and 775 victims IPs.
- In 2009, TWNCERT published totally 2,317 advisories, including:
  - Suspicious Attacks Warning: 1,878 (81%)
  - System Intrusion: 299(12%)
  - Website Defacement: 134 (5%)
  - Info. Security Message: 5(0.22%)
  - Critical Incident: 1(0.04%)



- In 2009, TWNCERT totally carried out e-mail social engineering drill (TrackRUSE Drill) to 39,158 individuals within 62 public sectors and results with Open Rate 22.3% and Clicking Rate 2.77%.

  TrackRUSE (Response under Social Engineering) system was developed to track individual end-user response under simulated social engineering campaigns. Social engineering drills were conducted using TrackRUSE system and drill results were shown to top management and those who had been tricked. This e-mail social engineering drill approach won Best Practices Contest 2008: Protect hosted by FIRST (Forum for Incident Response and Security Teams) and CERT/CC.
- In 2009, TWNCERT held 5 email social engineering workshops (TrackRUSE system introduction) including 134 people.
- In 2009, TWNCERT held 12 Government Information Security Conferences and 3 Information security internal audit trainings.
- In 2009, TWNCERT help 20 people finished CISM training and assisted 43 people to get SSCP training

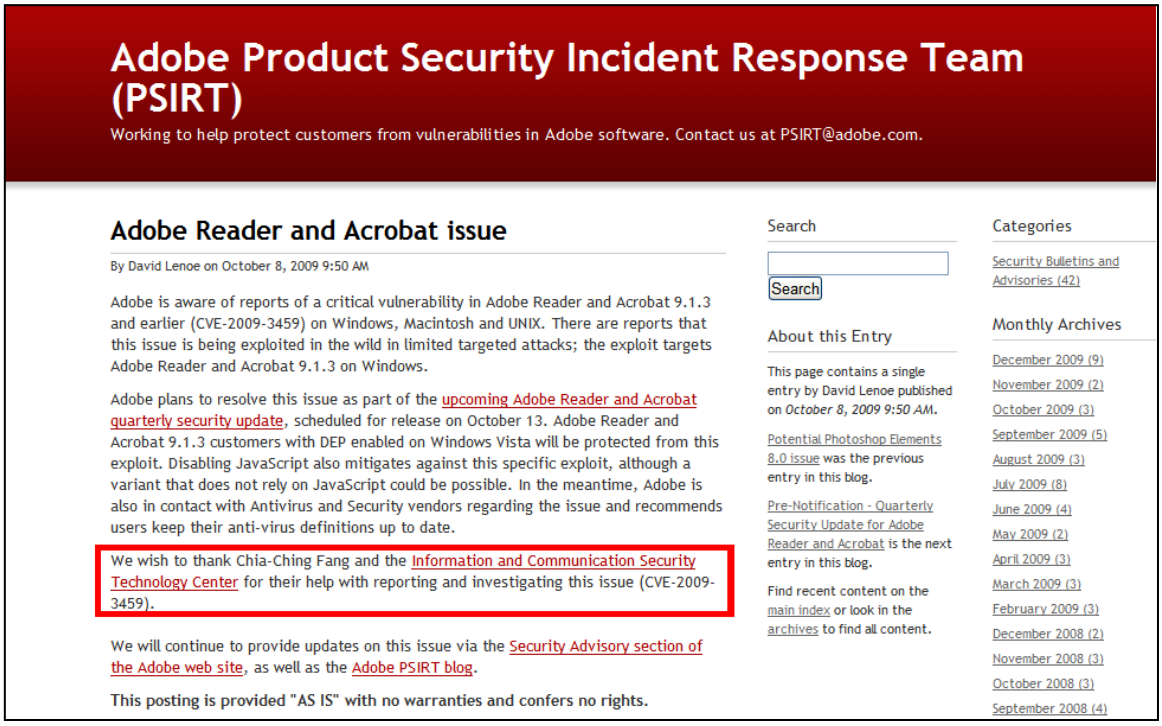
- 2009 Information Security Contest (including Catch-the Flag, Slogan, Poster and Animation Contest) starts from September to November.
  - Animation Contest: 406 attendees, 71 animation competitions and 10 winners.
  - Catch-the Flag: 139 attendees and 12 winners.
  - Slogan Contest: 2,234 competitions and 5 winners
  - Poster Contest: 141 competitions and 9 winners
- In 2009, TWNCERT propose a system called G-ISAC (Government Information Sharing and Analysis Center). TWNCERT will together G-ISAC members (TANet ISAC, Telcom ISAC and GSN ISAC etc) to sharing and info. Security intelligence.

3. Events

- Attended APCERT 2009 as the member in March 2009.
- Attended FIRST 2009 as the member in June 2009.
- Attended AVAR 2009 as the member in November 98/11

4. Achievements

- 2009/10/1, TWNCERT first found Adobe Reader/Acrobat zero-day attacks (CVE-2009-3459)。It is the 8th time that TWNCERT find the zero-day attack/vulnerability.



5. International Collaboration

- In 2009, TWNCERT totally received more than 732 international information security incident reports. Assisted and cooperated with other CSIRTs and governments.
- 2009/8, TWNCERT signed Cross License Agreement with MarkMonitor Inc. to cooperated email spam issue.
- Renewed the MOU between JPCERT/CC and TWNCERT in 2009/4.

15. VNCERT Activity Report

Vietnam Computer Emergency Response Team - Vietnam

1. About VNCERT

1.1. Introduction

VNCERT is an agency under Ministry of Information and Communications of Vietnam, established by decision of Vietnam's Prime minister in December, 2005. In Vietnam, VNCERT is responsible for state management of information security area.

Roles of VNCERT:

- Coordinating national computer incident response activities.
- Watching and warning computer network security problems.
- Building and co-ordinating to build computer network security technical standard.
- Promoting to build CERTs in the organizations, enterprises, and agencies in Vietnam.
- VNCERT is the point of contact of Vietnam with the oversea CERTs in this area.
- Support Ministry of Information and Communications with activities in state management about Information Security.
- Lead the process of deploy the Anti-spam Law (Decree No.90 of the year 2008) in Vietnam.

1.2. Staff and structure

VNCERT has four specialized divisions: Division of Operation, Division of System technique, Division of Training & Consultancy and Division of Research and Development. VNCERT also has two branches, one in Ho Chi Minh city and another in Da Nang city.

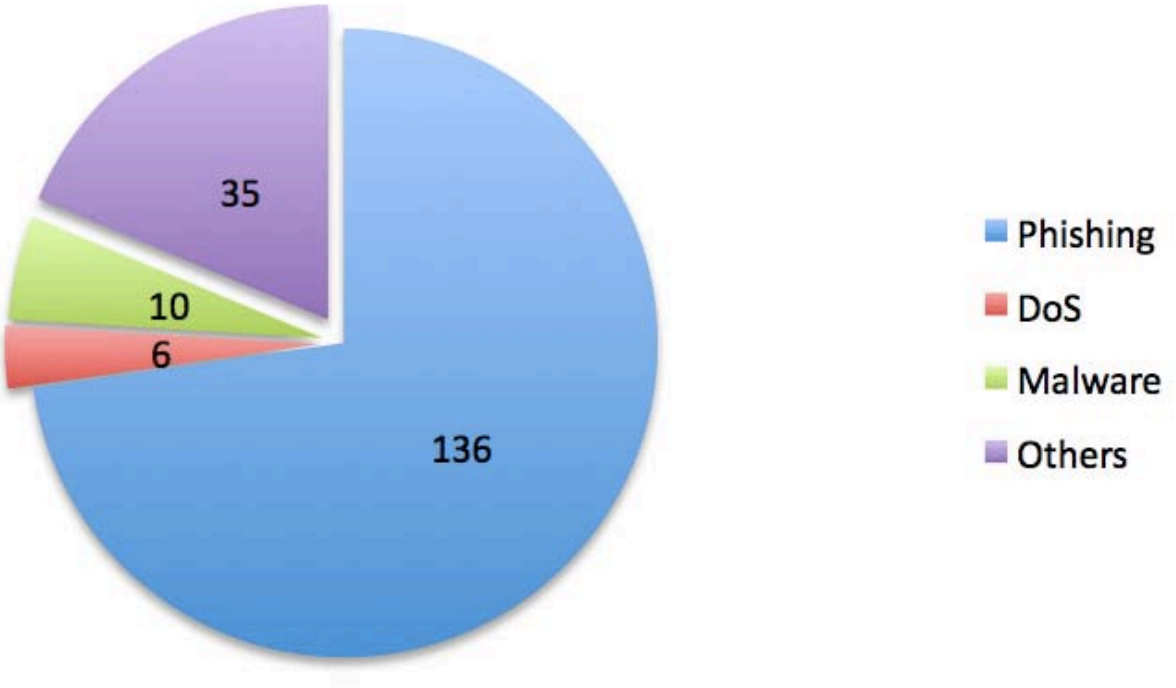
Current number of employees in VNCERT is about fifty.

2. Activities & Operations

2.1. Incident reports & handling

In 2009, the total number of serious incidents reported to VNCERT was 187, which has increased more than 100% in comparison with 2008. VNCERT had worked very actively in direct in handling of 169 incidents and had taken part

in 18 incident handling consultancy cases. Many reports were about phishing and malware as well as spam sources, some about DoS attacks. Almost phishing cases were related to finance, commonly forging banks' website to steal bank's account, and they were reported from outside Vietnam.



In 2009 there are 02 serious incidents in Viet Nam: the Conficker malware threat - Vietnam was in the top of infected countries; and a big search engine in Vietnam lost control their domain. Some incidents occurred on government agency systems, were handled by VNCERT quickly.

2.2. Watching and supporting activities

VNCERT also actively watched security news from many sources, and warned about security threats to organizations via private channels or to Internet users via media press. For examples, the threat of Conficker worm and some vulnerabilities of Microsoft products were warned early and widely.
VNCERT has supported some state organizations and industries to audit critical information systems and enhance system security.
VNCERT helped to secure all online important government events.

2.3. Anti-spam activities

- Published and deployed Decree 90/2008, Circular 12/2008, Circular 03/2009 to prevent spam messages.
- VNCERT has issued 50 certificates to Content Provider for providing advertising services on SMS, email and SMS over Internet.
- VNCERT has co-operated with Ministry Inspectorate to fine some companies that violated Anti-spam Law. At the end of the year, the number of spam messages decreased a lot.

2.4. Legal environment improvement

- Co-operated in building "Master plan for national developing digital information security of Vietnam in period from 2010 to 2020".
- Took part in editing 02 Decrees, 05 Circular to improve law system.
- Issued national standard TCVN ISO/IEC 27001:2009 ISO/IEC 27001:2005

3. Events organized / Co-organized

3.1. Training & Drills

- In 2009, VNCERT arranged some training courses for raising information security awareness as well as working experience in Information Security field to staff in some organizations.
- VNCERT participated in 02 international drills: ASEAN CERTs Incident Drill (ACID 2009) and APCERT Annual Drill 2010.
- VNCERT coordinated to organize IS contest between the students of 8 universities in Vietnam.
- Co-organized with VNISA and JPCERT/CC to provide CSIRT training.
- Co-organized with JPCERT/CC to organize the training course "Secure Coding".

3.2. Seminars & Etc

- Co-operated with Ministry of Public Security and IDG Vietnam Corporation to organize annual event "Security World", the largest IT security conference in Vietnam. The conference delivered leading-edge insights, compelling presentations and extensive opportunities to exchange ideas on how to develop effective security strategies and enhance business continuity.

- Co-operated with VNISA to organize successfully an conference related e-government and to organize the annual event "National Information Security Day 2009", the biggest and most important security conference of the year. The event was hosted by Ministry of Information and Communication. Main theme of 2009's is "Protect information asset today for the tomorrow growth!".
- Co-organized the first CSO Conference & Awards, featuring the theme "Security Leadership: Adding values to higher business performance", brought an overview of the information security market in 2009 as well as analysis and predictions of information security's needs in 2010.

3.3. Consultancy

VNCERT supported the state and private organizations in the IS area and helped the Government to develop the national strategy to secure cyber-space. Besides, VNCERT provided assessment service to a local bank, helped them in auditing their system and procedures.

4. Achievements

VNCERT:

- Took part in the national and international conferences related IS, VNCERT always made detailed reports on network security, actively expressed the idea and enthusiasm to the conference programs.
- Had a good communication with the press and other means of communication to inform the VNCERT's activities to the public, aiming to raise prestige and state management role of Ministry of Information and Communication.
- Deployed RD project on building Internet information security monitoring and management system, support in watching and early warning about information security threats.
- Published state macro-management model of the email-spam and SMS spam to the law system, took part in organizing activities to prevent spam messages.

5. International Collaboration

- VNCERT has signed MoUs with JPCERT/CC and KISA for co-operation in the area of cyber security.

- Co-operated with KISDI, Korea within the framework of a consultancy project of Korea related security policies building in Vietnam.
- Co-operated with oversea organizations to exchange experiences, study new technology and product that used for network monitoring.
- VNCERT has joined annual conference of APCERT, national CERTs conference, and many others.
- VNCERT has signed MoM with DTI of Laos for supporting LaoCERT; and had supported Laos to protect information service of Seagames 25.

Active international cooperation relationships help VNCERT to learn experiences, knowledge, and to reach promptly the regional and international standard related IS.

6. Future Plans

VNCERT will:

- Participate to deploy the "Master plan of national developing digital information security of Vietnam in period from 2010 to 2020", in the roadmap from now to 2020, national budget is expected to allocate 765 billion VND for 6 major projects which are given as top priority in setting up the laws and technical infrastructure for national security.
- Adjust some policies in law system for better suiting with current context.
- Develope and publish some new national standards on information security management and build up the National Network Security Technical Center in VNCERT.
- Strengthen information channels to deliver and receive cyber security information nation-wide.
- Organize the national workshops/events on cyber security.
- Continue improving official websites of VNCERT for cyber security and for anti-spam management
- Continue the RD projects on building the technical system for watch, warning and incident response and taking part in some international collaboration research projects.
- Participate actively in the collaboration activities among APCERT and ASEAN CERTs, improving exchange experiences activities; support LaoCERT.

- Take part in cyber security activities following co-operation framework of ITU and IMPACT.

7. Conclusion

As a Full Member of APCERT, VNCERT will do the best to fulfill all the responsibility to develop information sharing and cooperation framework within APCERT, aiming to improve Internet security level and the quality of Internet related emergency response in the Asia Pacific region, as well as to contribute to the world's information security development.

Particularly, VNCERT will fully participate in sharing data, research, response strategies, and early warning notifications with all other CERTs around the world.

Ministry of Information and Communication of Vietnam is willing to support the APCERT initiative and promise to support VNCERT to contribute actively to the activities of the APCERT.

General Members

16. BDCERT Activity Report

Bangladesh Computer Emergency Response Team - Bangladesh

1. ABOUT BDCERT

1.1. Introduction

BDCERT is the Computer Emergency Response Team for Bangladesh and is the primary Point of Contact for handling incidents from Bangladesh networks. We work for improving Internet security for Bangladeshi Internet users.

We provide information about threats and vulnerabilities that could affect the users. We work closely with various organizations and associations such as ISPAB, BASIS, BCS, SANOG, BTRC and Law Enforcement Agencies to stop attacks that are either sourced from Bangladesh or outside.

We help to mitigate Internet attacks directed at Bangladesh Internet users and networks.
We provide training and awareness programs on Information Security and issues affecting Internet security in Bangladesh and globally.

1.2. Establishment

BDCERT was formed on July 2007 and started Incident Response on 15th November 2007. BDCERT is initiated by some IT professionals who have long experience in data and Internet communication and technologies industry. It is funded voluntarily with limited resource but highly motivated professionals.

1.3. Workforce power

We currently have a working group of 12 professionals from ISP, Telecommunication, Vendors, University, Media, Bangladesh Internet Exchange (BDIX) & International Internet Gateway (IIG) who are working voluntarily with great enthusiasm and motivation. Some of the major activities that we are involved with, are, Incident Handling, National POC for

national and international incident handling, Security Awareness program, Training & Workshops, New Letters, Traffic Analysis, etc.

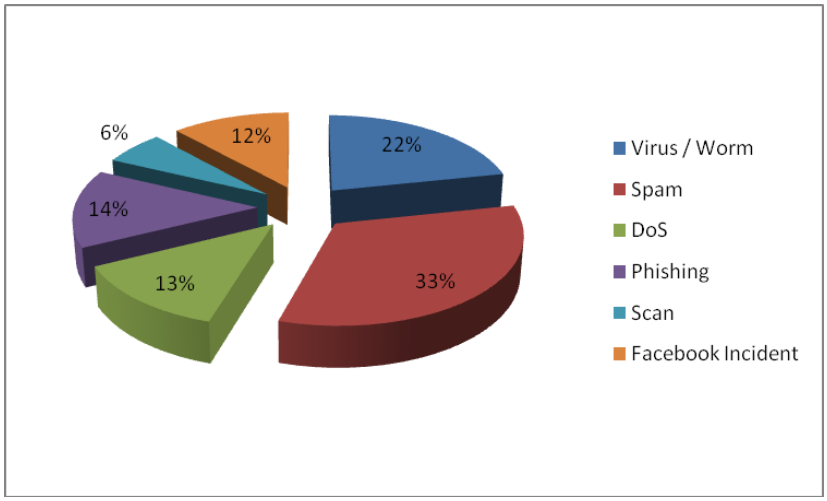
1.4. Constituency

As a national CERT the constituencies of BDCERT are all the Internet users of Bangladesh. We work closely with all the ICT stake holders particularly with ISP Association of Bangladesh (ISPAB), Bangladesh Association of Software & Information Service (BASIS), Bangladesh Computer Samity (BCS), Bangladesh Computer Council (BCC), Bangladesh Telecommunication Regulatory Commission (BTRC) and various Government Organization, Non Government Organization, Universities and Government Law Enforcement Agencies to mitigate Internet threats.

2. ACTIVITIES & OPERATIONS

2.1. Incident handling reports & Abuse Statistics

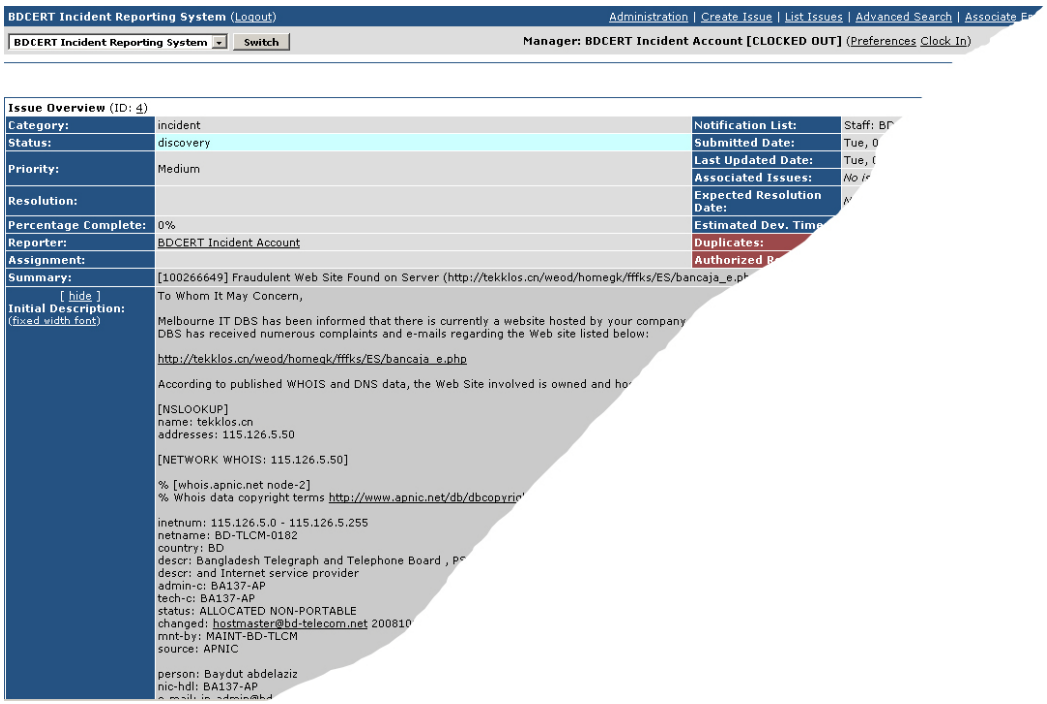
In year 2009, BDCERT has received 161 incidents reports. Taxonomy statistics of incidents report are shown in figure 1. Majority of incidents are related with spam and spam like email.



Taxonomy	Incident No
Virus / Worm	35
Spam	53
DoS	21
Phishing	23
Scan	10
Facebook Incident	19

Figure 1 : Taxonomy statics of Incident Response.

2.2. Online Incident Reporting System



SMS Based Incident Reporting:

3. EVENTS ORGANIZED / CO-ORGANIZED

3.1. Trainings & Seminars Organized

BDCERT have successfully organized various Information Security training, workshops and seminars with sponsors from various Government and Private Organizations.

- 13-14 June 2009: Cyber Crime Trend, Police Preparation and investigation Basic

  BDCERT member participate in the training session on "Cyber Crime Trend, Police Preparation and investigation Basic" organized by ITMAB. BDCERT member took session on "Digital Forensic".

- 13-16 May 2009: ISPAB DIGITAL MARCH 2009.

  BDCERT collaborated with ISP Association of Bangladesh (ISPAB) to arrange "ISPAB Digital March 2009". ISPAB Digital March 2009 was a 4-day (13-16 May) nationwide digital rally for raising internet awareness, information security awareness and celebrating World Telecommunication and Information Society Day (WTISD)-2009. Mr. Dilip Barua, Minister of Industries and Brig Gen Zia Ahmed, psc (Retd.), Chairman Bangladesh Telecommunication Regulatory Commission (BTRC) inaugurated the event.

  A fleet of 10 microbuses with mobile VSAT, high tech digital gadgets and logistics escorted industry IT experts from Dhaka to Chittagong. Four (04) schools were visited to show case technology and take short lessons on Internet and Cyber Security to young students in the country side.

- 13th May - Comilla Zila School. More than 600 students from various schools attended the event.

- 14th May - Bolakhal J N High School & Vocational College – over 200 students participated with keen interest.

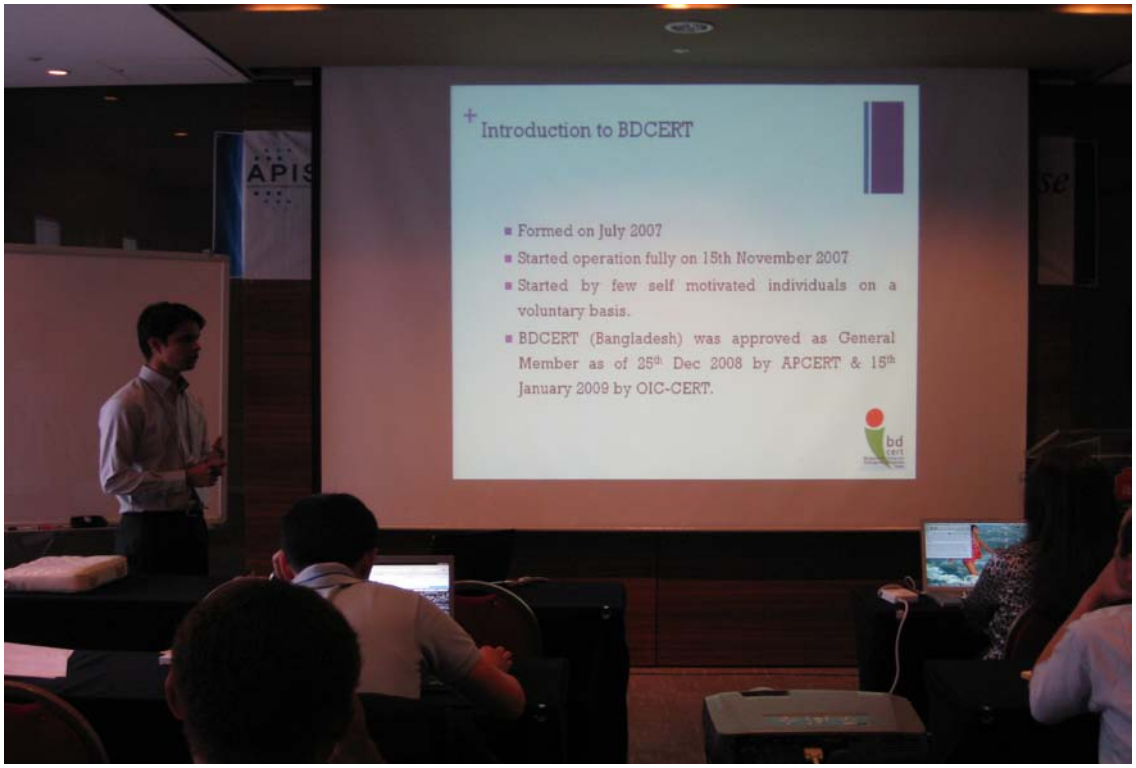
- 14th May - Chandpur Club Auditorium. More than 300 students from various schools attended the event to learn about Internet and internet security.

- 16th May Chittagong Muslim Education Society High School – more than 100 students were given short lessons on Internet and Cyber Security.

- 17-18 May 2009: World Telecommunication and Information Society Day (WTISD) 2009
  - Bangladesh Telecommunication Regulatory Commission (BTRC) organized a 2 day event at Chittagong Engineering Institute (IEB) to celebrate World Telecommunication and Information Society Day (WTISD) 2009. The event constituted Fair, Essay & Illustration Competition, School Quiz Competition on ICT Knowledge Base, etc. BDCERT Chair Mr Sumon Ahmed Sabbir spoke on the ITUs' theme of the year "Protecting Children in Cyberspace".

3.2. Trainings & Seminars Participated

- 11 - 15 May 2009 - 2009 Asia Pacific Information Security Center (APISC) Security Training workshop held at Korea, supported by KrCERT/CC.



4. ACHIEVEMENTS

- Successfully participated in ISPAB Digital March 2009. BDCERT team delivered special tutorial for government high schools at Comilla, Chandpur and Chittagong. Over 1000 students participated to learn about Internet and its safe usage.
- Supported WTISD 2009 fair organized by BTRC. Special speech and write up supporting ITU's theme of the year "Protecting children in the cyberspace".
- Successfully conducted "Digital Forensic" training as part of "Cyber Crime Trend, Police Preparation and investigation Basic" organized by ITMAB. Law Enforcement Agencies have been the participant.

4.1. Presentation

BDCERT has given presentations at several conferences throughout 2009 which includes:

a) APISC 2009, hosted by KrCERT/CC
b) ISPAB Digital March 2009, hosted by ISPAB
c) Cyber Crime Trend, Police Preparation and investigation Basic organized by ITMAB.

4.2. Publication

The first edition of BDCERT News Bulletin was issued on March 2008. BDCERT also has awareness programs regularly published in the IT Magazines.

5. INTERNATIONAL COLLABORATION

BDCERT is collaborating with JPCERT/CC in Internet Traffic Monitoring Data Visualization Project "TSUBAME" project. In this project, sensors for the Internet traffic monitoring system are installed in the Asia Pacific region, and monitoring data acquired by these sensors are shared among participants of this project.

6. FUTURE PLANS & Projects

a) Government Endorsement for BDCERT
b) Full Membership of APCERT
c) Full Membership of OIC-CERT
d) Membership of FIRST
e) Fund Raising
f) Information Security Hands -on training with fresh University Graduates, Government Organizations and Banks and Financial Institutes.
g) Awareness Programs: Security Week to raise general awareness on basic information security.

7. Conclusion

Internet users are growing quite rapidly over the past 4 years, especially since Bangladesh got connected to the global submarine cable system SEA-ME-WE-4 in May 2006. Though we have huge growth in Telecommunication and Internet but cyber security is not very familiar to general people except the nuisance of viruses and malwares. Thus BDCERT is working hard to make people aware of risks of unsecured Internet. We are working closely with law enforcement agencies, government bodies and international CERTs to provide Incident response and mitigation to cyber threats.