APEC

Asia-Pacific
Economic Cooperation

Best Practice for cooperative response based on public and private partnership

Security and Prosperity Steering Group
APEC Telecommunications and Information Working Group

2008

TEL 01/2006 – Strengthening Effective Response Capabilities among APEC Member Economies

Prepared by
KrCERT/CC
Korea Information Security Agency
78 Garak-dong, Songpa-gu, Seoul
Korea 138-950
Tel: +82 2 405 5138, +82 2 405 5424
Fax: +82 2 405 5129
Email: cert@krcert.or.kr
Website: www.krcert.or.kr

For
APEC Secretariat
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 68919 600 Fax: (65) 68919 690
Email: info@apec.org Website: www.apec.org

APEC#208-TC-03.1

Contents

Executive Summary

Recent trend of Internet incident shows that the motivation for cyber attack is evolving to the financial gain, the victims are changing from the large anonymous to the particularly targeted and narrowed as well. Hence, this trend brought out the new schemes of cyber attack, by hackers to make them to be more successful and efficient, by taking advantage of emerging bot, phishing, and malware to be installed to vulnerable computers. These malwares[1] are in the consistently increasing state in recent years, and the responsible organizations such as national CSIRTs are eagerly seeking the appropriate solutions for mitigation of newly arisen threats.

Bot is usually a bigger threat when it becomes more than two, particularly called as "botnet," in which a great number of computers are compromised, many unknown to the computer owner (these are termed "zombies"), and the botnet controller utilises them for malicious activities; spam relay, phishing host, and distributed denial of service attack including even to the system that acts to try to block the botnet activity, as retaliation.

This document mainly focuses on the system models, herein introduced, that can possibly be adopted by CSIRTs, including the national level CSIRT who acts as an overall coordinator for nation-wide major incidents and/or the CSIRT that has a relatively large scale of constituency, to mitigate malicious network activities in Internet involving various malware such as a bot, which is commonly recognized by security experts as a challenge to mitigate or overcome, therefore the introduced models herein can provide efficient and proactive ways to take action and response against those malicious activities, within the perspective of public and private partnership. This document also introduces the recent trends of APEC member economies who participated in the training course for building up and operation of CSIRT, including their activities and efforts to mitigate the Internet threats they face and as part of a best practice initiative.

The purpose of this best practice is to contribute to the APEC member economies by providing system models that can bring ideas of what type of scheme could be better for their environment of Internet threat regarding the circumstances and issues that may reside at the moment.

[1] A software designed to infiltrate or damage a computer system without the owner's informed consent

1. Introduction

1-1. Background

The project “Strengthening Effective Response Capabilities among APEC Economies” is for each APEC economy, including the developing economy, to have its own response capabilities for the Internet incidents. After many member economies began recognizing the importance and needs of CERT[2]/CSIRT[3], some of APEC member economies, including the developing economies, are promoting the establishment of CERT/CSIRT. Many economies do not have the capabilities of helping other CERTs' establishment and management.

To assist the APEC economies building the response capabilities, the project will provide the training course and develop guideline and best practice. The short-term training course is offered for other CERTs in APEC economies to have the opportunity to learn the methods and issues which should be considered during the establishment and management of a new CERT. The objective of the short-term training course is for the participants to have the capabilities to train other Information Technology or Information Security staffs for the establishment and management of CERT from the business and technology perspectives. The cooperative response guidelines in cross-border environment will be the referential material for international incident handling for major cyber incidents. Although most of CERTs have the internal process for the local incident handling, most of CERTs may not have any standardized process or referential material for cross-border or international incident handling. The previous experience of international incident handling drill will be the basis of the guidelines and the guideline will be drafted and revised with the discussion with CERTs in Asia Pacific Region. The best practices for cooperative response based on public and private partnership will be another referential material for developing the local response system, including network operators.

The project is partially funded by the Operational Account of the APEC Central Fund. The short-term training course is being organized by KrCERT/CC, a division of KISA, with the cooperation from FIRST[4] and TERENA[5] which provides the certified trainers for courses and training materials. This best practice is developed by the KrCERT/CC with the help from the staff who can advise and review of the content in the technical and non-technical perspectives.

1-2. Purpose of Project

The main objectives of this project are to enhance the APEC economies' response capabilities. From the local perspectives, promoting the establishment of CERT and the cooperation among the stakeholders such as ISPs[6], MSSPs[7] and vendors is the key factor. As well from the international perspective, the cooperation among cross-border

[2] Computer Emergency Response Team, an organization dealing with Internet security

[3] Computer Security Incident Response Team, generic term of CERT

[4] Forum of Incident Response and Security Team

[5] Trans European Research and Education Network Association

[6] Internet Service Provider, an organization that offers users access to the Internet and related services

[7] Managed Security Service Provider, who provide security services for companies

CERTs would be the key factor.

All these activities can be integrated into one of APEC-TEL efforts on information security to make knowledge-based economies prosper. This project will contribute to make APEC economies secure by promoting CERT building and the cross-border CERT cooperation.

2. Cooperative response based on public and private partnership

2-1. Establishing the National Network Monitoring System with Cooperation from Domestic ISPs

At 25 January 2003, Korea had a critical Internet service break-down for a quite amount of time, which caused critical infrastructure to have serious damage by inability of providing the services including financial sector, logistics, and almost all critical infrastructures. Also the actual monetary loss affecting the national economic growth by the break-down was enormous. This was an awakening happening for all the citizens, and a greater impact to people who were managing and responsible for the Internet infrastructure, to Internet service providers, IT experts, government officials, and every relevant stakeholders. Before this major crisis, there actually was no well-established systematic network monitoring infrastructure for nation-wide Internet environment. It was a reactive response scheme that the incident handlers take the incident from the reporter, through the phone calls and emails received, which means that it is already happened, and take an appropriate action to those victim systems for mitigating the further damage.

This case led the related experts to feel the need to have a preventive measure against the major Internet threats and incidents. To take an immediate action and maximum mitigation for critical cyber incidents, real time network monitoring at nation-wide level is essential. To make it possible, institutional and jurisdictional backup is also essential.

Korea has the law that supports the nation-wide network monitoring can be attained. The law says that every major information service providers related with provision of information network service and those businesses with relevant facilities should provide computer incident related information such as statistical information of their network and such information assorted by communication channels. In detail, those are statistical data of the Internet traffic volume by nodes, ports, protocols, and attack types on their network, and no payload data are collected whatsoever.

As of October 2007, KrCERT/CC is monitoring over 94% of the domestic IP, with the cooperation from the major local ISPs. Business sectors providing their data other than ISP are, IDC[8], SO[9], MSSP[10], anti-virus vendor, portal site, online game company, and academy. With this huge amount of data, KrCERT/CC is able to perform the analysis on the daily Internet traffic inbound and outbound to Korea, and detect abnormal patterns to be able to take appropriate action for early warning system, to benefit and protect nation-wide Internet infrastructure.

A server is to be resided in the physical location of the organization that provides the statistical data to KrCERT/CC. This server would then only collects traffic data explained above, and forward these data through dedicated line or VPN[11] by every 5 minutes basis. In the end of these lines, a collection server is needed to collect and

[8] Internet Data Center, a facility used to house computer systems and associated components normally connected to Internet

[9] System Operator, regional cable TV business providing Internet service

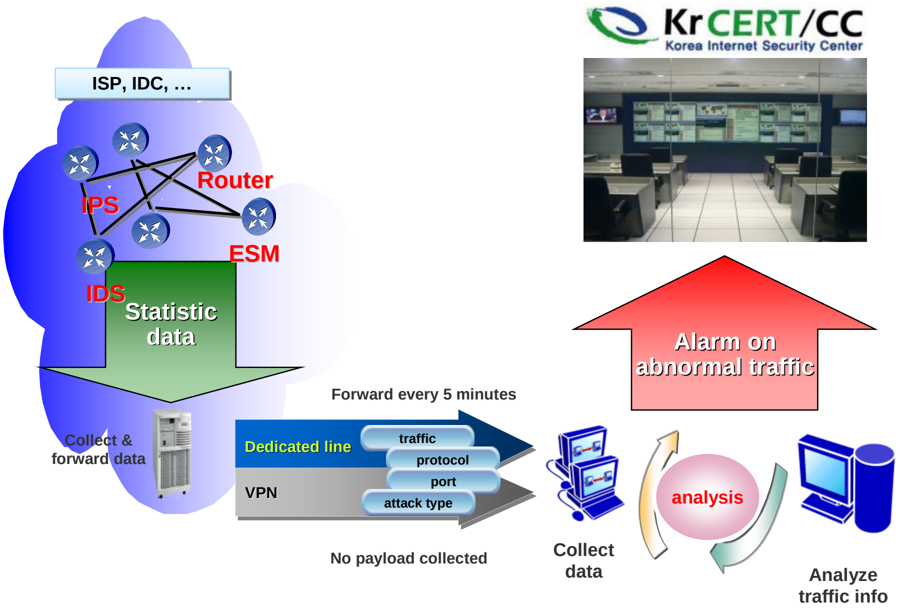
[10] Managed Security Service Provider, who provide security services for companies

[11] Virtual Private Network, a communications network tunneled through another network, and dedicated for a specific network

manage the data to make ease of the analysis and display. An operator can then recognize the abnormal traffic as the system tells when such traffic peak happens, in audio-visual way.

Relevant Act for Network Monitoring

Article 48-2 (Response, etc. to Infringement Accident) (1) The Minister of Information and Communication shall perform the task falling under each of the following subparagraphs to properly cope with any infringement accident and may, if necessary, get the Security Agency to perform the task, in whole or in part:
1.The collection and dissemination of information on infringement accident;
2.The forecast and alert of infringement accident;
3.Emergency measures against infringement accident; and
4.Other measures prescribed by the Presidential Decree to cope with infringement accident.
(2) The person falling under each of the following subparagraphs shall furnish information pertaining to infringement accident, including the statistics of infringement accident by type, the statistics of traffic volume in the relevant information and communications networks and the statistics of uses by connection channel, to the Minister of Information and Communication or the Security Agency under the conditions as prescribed by the Ordinance of the Ministry of Information and Communication:
1.The provider of major information and communications services;
2.The business operator of agglomerated information and communications facilities; and
3.Other person who is prescribed by the Presidential Decree as the operator of the information and communications networks.



Flow of Network Monitoring

Implication summary

National network monitoring is a challenge.

Establishing or implementing a nationwide network monitoring system should obviously be a huge challenge for any economy. Not to mention the necessity of legal support, cooperation and understanding among the stakeholders are the viable value needed to be able to make it feasible.

Mutual benefit

The benefit from establishing the national network monitoring should be applied to all stakeholders, including general users to Internet service providers. If an authority should be the focal point for network monitoring, overall benefit from this after establishing the keen cooperation would satisfy social and economical aspects. This can prevent general public from involving in the malicious activity, thus can minimize the damage caused in the economy.

Cooperation essential among stakeholders

Most important entities in this practice could be the Internet service providers. An institution or government responsible for building up this system should adopt the manner of close cooperation to discuss with the stakeholders and may go through a tedious debate for mutual understanding. It is rather a structure once the initial step of the setup has been completed.

Budget

Appropriate budget should be considered by the initiative and need to be readjusted as it expands its scope or objective of the nationwide network monitoring system.

Privacy

One of the most important criteria on this is privacy concern. Under the jurisdiction of the economy, the data collected by the established system shall not provide a cause of infringement of the rights of the juridical and natural person.

2-2. Establishing the Botnet DNS Sinkhole System with Cooperation from Domestic ISPs (Countermeasure for Botnet Handling)

Bot is an amorphous malware evolving over time and adjusting itself with integrating all possible malicious functions according to the herder's[12] needs. Botnet usually consists of Botnet C&C (Command and Control) server and bot-infected zombies. Botnet C&C server is an intermediate server which bot herder or hacker sends command and control messages for bot-infected zombies to execute malicious activities, such as DDoS (Distributed Denial of Service), collecting classified or financial information, mass spamming, and etc.

Botnet C&C servers commonly make use of IRC (Internet Relay Chat) communication channel to operate and some of them are adopting the encryption in the communication between C&C server and zombies to prevent being identified. Interestingly, Botnet C&C servers usually use the dynamic DNS name, no static IP, since Bot herder can modify the IP configuration of Botnet C&C servers once that server IP is identified and blocked. A Botnet C&C server has a DNS name, e.g. botnetcnc.net. If PCs are infected with some kind of malicious bot, zombie PCs would make DNS queries to obtain the real IP of C&C servers to make connections to and wait for commands from C&C servers.

The sinkhole system is to prevent zombies' connections to Botnet C&C servers, by deceiving the IP of Botnet C&C server. When bot-infected zombies make a DNS RR[13] queries to DNS server in the network operators, such as ISPs, which zombie PCs are resided in, the answer to query (IP address for the Botnet C&C server) will be an IP of the sinkhole system. The connection attempt will be redirected to the sinkhole system in KrCERT/CC, not to the Botnet C&C server. Although zombies think they are connected to Botnet C&C server, the connection is made with the sinkhole system. Because zombies have lost connections with Botnet C&C server to receive the command and control, malicious activities are stopped. Sinkhole system can track and analyze all activities of Botnet zombies connected.

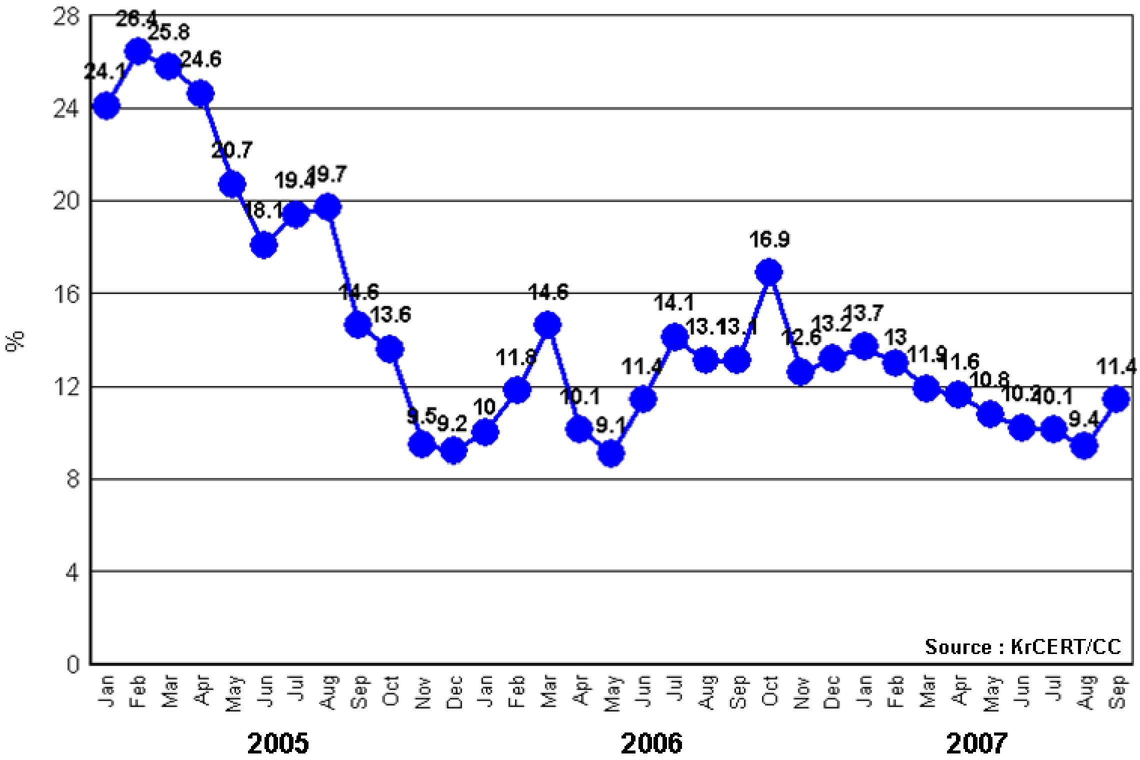
KrCERT/CC provides Botnet C&C server information collected from various sources after the validity checkup of the information to participating ISPs consisting of most of domestic major ISPs and some of small and medium sized ISPs. The Botnet C&C server information is not limited to foreign servers. Participating ISPs apply those DNS zone files to their own DNS servers. This makes Korean users protected from Botnet threats.

After the adoption of this sinkhole system in 2005, the Botnet infection rate of Korea dropped to almost one third in the end of 2005, compared with that of January or February.

[12] Bot herder is a person or persons who use automated techniques to scan specific network ranges and find vulnerable systems

[13] DNS Resource Records: An alphabetical list of resource records used for Internet domain names

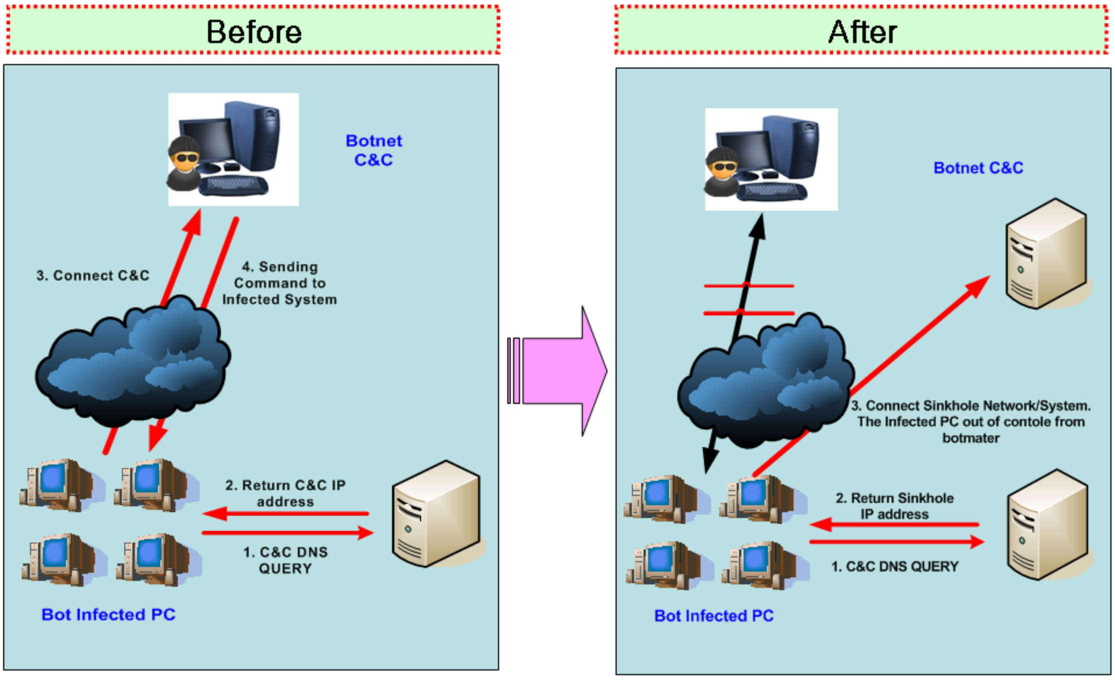
Bot Infection Rate of Korea (2005-2007)



Source : KrCERT/CC

To Build Up DNS Sinkhole System

- Purpose
  - To remove the malicious sites and to decrease the damage caused by hacking


Before
Botnet C&C
3. Connect C&C
4. Sending Command to Infected System
2. Return C&C IP address
1. C&C DNS QUERY
Bot Infected PC
After
Botnet C&C
3. Connect Sinkhole Network/System. The Infected PC out of contole from botmater
2. Return Sinkhole IP address
1. C&C DNS QUERY
Bot Infected PC

- Effect
  - Prevent connecting to Bot C&C server and malicious code distribution site
  - Decrease abused internet traffic
  - Decrease DDoS attack

Considerations

- Reconfiguring DNS may cause delay of service, but it only takes 1-2 seconds, so it is rather a small effect to DNS service.
  - In Korea, already more than 9 ISPs are running the DNS Sinkhole, so stability was verified.

- There are several check points as following;
  - DNS reconfiguration flow may cause error, so DNS operator must observe the reconfigure process. It may increase operator's workload.
  - When reconfiguring DNS, it takes 1-2 seconds, and during that period DNS cannot respond.
  - The black list domain must contain unique domain list. If there are overlapping domains, DNS may cause error.

- The sinkhole network can be an attacking target by hackers. Bot herders can find out why their bots cannot connect to Bot C&C, and Bot herders can eventually find out the existence of Bot DNS Sinkhole network. Therefore, a DNS sinkhole itself can be attacked by hackers.

- If many ISPs participate in the DNS Sinkhole projects, bandwidth of the sinkhole network must be sew up.
  - However, even when a sinkhole network goes down, there is no problem for ISP. The zombie PCs would just try to connect to the sinkhole network and do nothing.

Implication summary

Enhancing response capability

Proactive response system is crucial to enhance more efficient Internet incident response capability. DNS sinkhole system is one of the finest ideas that can be applied in the network level with pre-established system to protect users from malicious activities.

Reliable source

A reliable source that can provide malicious domain or IP is to be prepared to make the sinkhole system operate and fully utilize. Honeypot/honeynet could be the one of the good measures that can collect the malicious entity information. However, establishing a honeypot/honeynet causes some amount of budget in any scale, so using a help through cooperation with the organizations who provide resources of malicious entities. There are many organizations putting much effort to make Internet more secure, and that can provide the information on those malicious activities.

Public private partnership

Applying a sinkhole in the network is not technically challenging, rather establishing a concrete partnership with the relevant stakeholders is more challenging. Nationwide DNS sinkholing is, of course, requires a lot of efforts not only for the coordinator, but also between the sectors of public and private when the benefit of the general public is to be sought.

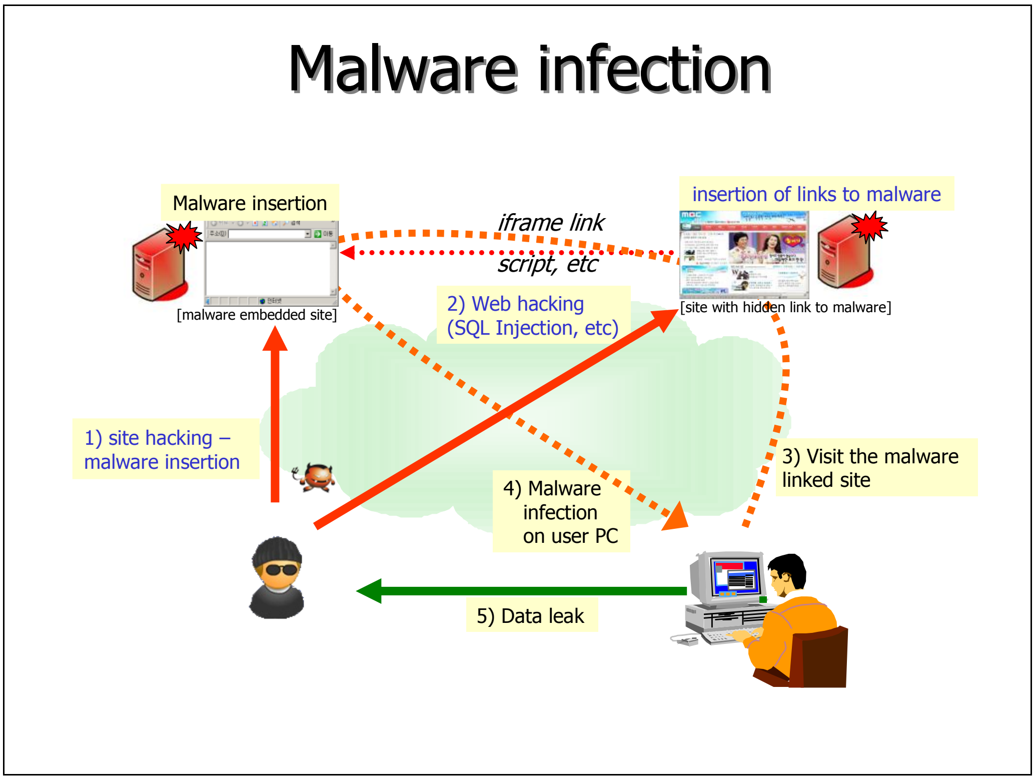
2-3. Provision of Malicious Code Finder

Recent hacking trend is evolving to focusing on application layer, and the mostly increasing attack is targeting for websites which relatively easy to hack and the impact is huge.

Webpage defacement used to be a hacker's sport, but the recent trend is that they inject a malicious code in a hidden place of the vulnerable computers. This makes users and server administrators unaware of the fact that they are hacked, in visual way, contrary to webpage defacement, moreover, users visiting the website are infected by the malicious code, and thus it causes additional damage.

Damage can be vary and caused by the breach of the login and personal financial information, and even developed to a serious DDoS attack targeting to a certain site. The DDoS attack recently occurred turns out that the website was involved as the source of the attack, which proved to be hacked and exploited with a Trojan that performs the attack to a website located in a foreign economy.

Typical malware infection can be described by the diagram below.

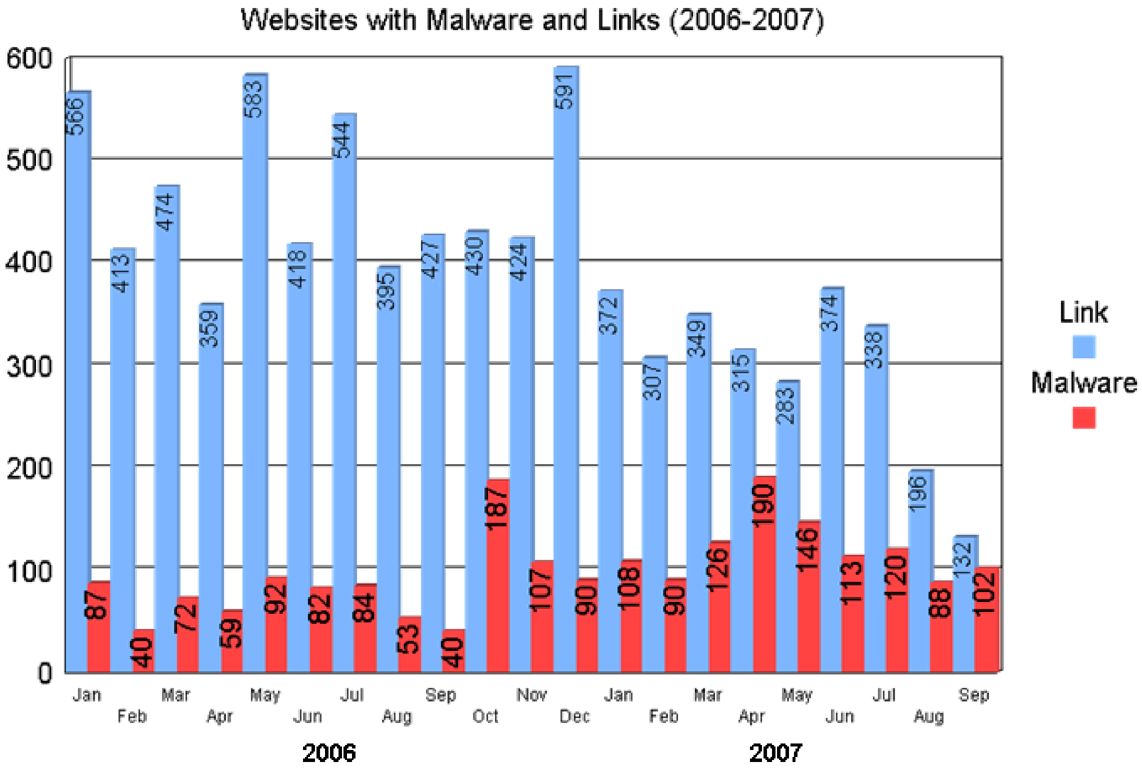


Basic countermeasure of installing and updating the anti-virus software is important to prevent from infection of the malware, but more important means for security is to block the distribution source which users have visited with no intention whatsoever.

KrCERT/CC in Korea has a detection tool called MCFinder[14], that is able to automatically search for a malware that hidden in the websites, and take actions to

[14] Malicious Code Finder

eliminate or to block the found malware website or the malware itself. KrCERT/CC detected over 500 compromised websites in average every month in 2006 among the subject sites using this tool, and this number of compromised sites is decreasing recently to around 200 as the MCFinder consistently detects the compromised sites, taking actions to raise the security level especially for the sites compromised repeatedly, thus the rate of re-infection seems to be dropping, as shown in the graph below.



A malware and/or the link to the malware can be inserted into a vulnerable website by hackers exploiting existing vulnerabilities of the HTML, javascript, and so on. Typical method of linking the malware can be done by using the iframe tag in HTML. Many other methods can be used to hide a link to the malware, so that the users cannot recognize that they are actually visiting, downloading, and executing the malware. MCFinder accumulates these methods into its database, and with these patterns it crawls and searches for a malware. It is a proactive response system which is the best advantage when adopting. Hence, it enables immediate handling for the compromised website, thus the damage can be minimized.

MCFinder engine has been distributed to over 100 domestic organizations in public and private sectors in Korea, including the law enforcement, major ISPs and MSSPs, telecommunication operators, media, online games, academic institutions, and so on, and it runs to protect their own constituency every minute.

KrCERT/CC also put a lot of effort for global users to have benefit from the outcome from this tool, by cooperating with a leading search engine company, Google, by mutual update by exchanging the patterns with each other.

Herein, a concept for adopting a DNS sinkhole system for the found malware distribution websites can be further considered and developed. Huge impact can be expected if an independent organization that operates a separate DNS server adopts DNS sinkhole system, which is able to prevent its own constituency from malware infection.

DNS sinkhole system is a specific technique for the malicious connection to be redirected and guided to the site, instead of the real site, which specifically established with the purpose of blocking the connection to a certain domain. Applying the sinkhole technique can prevent users from infection by the malware distribution site, and DDos attack to a network caused by the systems already infected by the malware.

In appendix A, we introduce how to apply and manage DNS sinkhole system for DNS server that runs in Windows OS, and for BIND[15] runs in UNIX and Linux systems.

Implication summary

Malware distribution by the web is growing

Malware distributed through the websites is a huge threat since Internet population is constantly growing and most of the users are using a web browser, which is a very powerful and convenient tool, and at the same time, very easy to be abused by hackers for malware distribution.

Finding a malware for constituency

Crawling and searching for malware in the multiple websites looking at each page can be explained as to perform a minimal remote inspection with the very short interval. It is a simple idea but very efficient. Network load caused by this is relatively low, even with the bigger size of the constituency. Of course, bigger constituency is a challenge for this kind of tool; triage can be adopted with a several criteria such as, the number of daily users, the importance of the sites, etc.

Good response system required

Facilitating a good response system for these incidents is more important than just detecting the malwares. Cooperation between public and private entities is needed to deliver/notify and feedback to take down every incidents.

[15] BIND (*Berkeley Internet Name Domain*) is the most commonly used DNS server on the Internet, especially on Unix-like systems, where it is a *de facto* standard.

2-4. Automated Security Update Program (ASUP) Development and Deployment

According to the survey on Internet Usage by NIDA, 75.5%[16] of Korean people use Internet for the work, fun, shopping and other various purposes. Internet became a part of usual life in Korea. Another broadband statistics from OECD shows that Korea is one of the highest broadband penetrated countries. Among the broadband users in Korea, more than 22% users are connected to Internet with FTTC or Fast Ethernet (100Mbps).

Hackers or malicious actors prefer PCs or servers resided at home or SMEs[17] with the broadband connection. With the small number of malware infected computers, hackers can initiate decisive attacks which can bring substantial damages to targets or victims. Most of those are vulnerable from the security perspective. Because home users or SME server administrators may not be aware of the basic concept of information security, the critical vulnerabilities in computers are left without taking any action to correct, such installing the patch or security software or hardware.

The recent trend of malware is that the exploitation of system software (operating software) vulnerabilities, especially Microsoft Windows, is increasing and even zero-day attacks, exploiting vulnerabilities with no patch or remedy released, occur more frequently. Windows vulnerabilities are exploited frequently, because Microsoft Windows monopoly in OS market (over 95% in Korean market) makes most computer users affected. Hackers are targeting Microsoft Windows vulnerabilities because it has the most extensive reach through Windows users and the exploitation of Windows is more efficient than that of any other software.

Most of the users may not be aware of the importance and necessity of patching for closing the hole in Windows. Blaster worm occurred in 2003 is a typical worm for exploiting the Windows vulnerabilities. Blaster worm has brought substantial damages around the globe. The continuous rebooting symptom after blaster worm infection made users recognize that their computers have a problem.

Comparative amount of malwares are propagated by spam email or exploiting the Windows vulnerabilities. More malwares are recently using stealth technique to hide the infection and existence within computers. Malware with scanning capability searches adjunct computers with Windows vulnerabilities which can be used as the door to get into the system and get the full administrative rights.

From year 2005, identity theft in major Korean online games became a major social issue and enormous reports on the robbery of online game items, which takes long time to obtain and can be exchanged to the real money, were filed to on-line game companies and law enforcement bodies. Malware to collect the personal information, exploiting Windows vulnerabilities to infect, was installed on computers of on-line game users, especially identity theft victims. Those users were not aware of what is malware, vulnerability or patch. Most of users did not install the patch to close the hole (vulnerability) of MS Windows.

To reduce the damage from those MS windows vulnerabilities, the most potential

[16] As of June 2007, http://isis.nida.or.kr/index_unssl.jsp

[17] Small and medium enterprises

targets of malware to exploit, KrCERT/CC and Microsoft Korea collaborated to develop and deploy the Automated Security Update Program (ASUP) to home and SME users. The program is to make all Internet connected PCs install security related patches without user intervention after the installation of ASUP. When users visit Korean major websites, such as portals, on-line game sites, a popup window to confirm the installation of the ASUP appears in the screen. After the installation, ASUP periodically checks up the new available Windows security patches and installs them without user's intervention. Although it has the same functionality with windows automatic updates, ASUP has some advantages. Users do not need to modify the configuration of windows updates but just to click once to approve ASUP installation.

KrCERT/CC has led efforts from the initial phase of development, such as the design of ASUP and deployment of the program to users, and encouraged online game sites and highly ranked sites, in the respect of number of visitors, to adopt this program that the site visitors can easily install this ASUP. Many of online game sites validate the installation of Windows patches to protect game users from malware infection.

Microsoft Korea has managed and distributed the program in accordance with Microsoft headquarters' centralized patch policy, balancing user convenience and company's philosophy on security.

Although the initial version was developed only for Windows XP in 2005, the new version has been developed to actively respond to technological advances in year 2006, with the release of Windows Vista.

Implication summary

Partnership with software vendor

This is the part that shows the importance of cooperation and partnership between public and major software vendor. To reduce the number of computers vulnerable, a fast recovery system for vulnerable computers is required. This can be accomplished through a centralized coordinator, e. g., a CSIRT, but by the efficient method such as distributing small software into every client computers. This should, of course, be agreed before installation.

Seamless update

Managing the software is more important matter, by updating its database of target vulnerabilities, and also to make itself safe from the known vulnerability and undiscovered.

Appendix A

Operational Manual for DNS Sinkhole System Management

How to apply and operate DNS sinkhole in UNIX/Linux

Assumptions

This manual is to apply sinkhole for UNIX/Linux DNS servers with bind 8.x/9.x environment, and assumes as such below for friendly explanatory.

- DNS server installation directory: /etc/namedb
- Sinkhole applied zone file: sinkhole.zone
- Domain configuration file for sinkhole of malware distribution site: sinkhole.conf

✓ Please check before applying to the installation directory for bind which differs for different operating systems. (Table 1 shows common directory names for various operating systems)
✓ “sinkhole.zone,” “sinkhole.conf” files should be provided.

A. System backup and recovery

For backup and recovery for DNS server in UNIX/Linux, compression/decompression method is used such that, the relevant directory is compressed and archived as “.tar” and so on, and decompressed when an error is encountered.

B. Configure and apply DNS sinkhole

Step 1. Move to the DNS server installation directory for configuration

```
prompt# cd /etc/namedb/    →    installation directory for name server
prompt# _
```

Step 2. Create the zone file for applying to sinkhole

Zone file provided can be copied to the directory /etc/namedb/.

```
prompt# vi sinkhole.zone    □   create zone file of domains for sinkholing
```

```
$TTL 600
@       IN      SOA localhost root (
                        2007051301      ; serial
                        3600            ; refresh after 1 hour
                        1800            ; retry after 30 min
                        1W              ; expire after 1 week
                        600 )           ; minimum TTL of 1 hour
IN      NS      localhost
;; Static Address for NS Server
ns      IN      A       127.0.0.1
;; Server
```

Step 3. Add the filename “sinkhole.conf”, that contains domain names of malware distribution site, to the “named.conf”.

```
prompt# vi named.conf
                                        · · ·
include "sinkhole.conf";
```

Step 4. Configure the applied domain zone by malware distribution domains

“sinkhole.conf” file provided can be copied to the directory /etc/namedb/.

```
// example of applying sink1.x.net, sink2.x.com into sinkhole
zone "sink1.x.net" IN { type master; file "sinkhole.zone"; };
zone "sink2.x.com" IN { type master; file "sinkhole.zone"; };
                                        · · ·
```

Step 5. Update information for DNS

```
BIND 8.X version: prompt# rdc reconfig
BIND 9.X version: prompt# rndc reconfig
```

<Table 1> Common installation directory by operating systems

OS version	BIND 8	BIND 9
Redhat	/var/named /etc/named /etc/namedb	/var/named /etc/named /etc/namedb
Fedora	/var/named /etc/named /etc/namedb	/var/named /etc/named /etc/namedb
CentOS	/var/named /etc/named /etc/namedb	/var/named /etc/named /etc/namedb
Gentoo	/etc/bind	/etc/bind
Ubuntu	/etc/bind	/etc/bind
Debian	/etc/bind	/etc/bind
Slackware	/var/named	/var/named
Mandriva	/var/lib/named	/var/lib/named
SUSE	/var/lib/named	/var/lib/named
Solaris	/var/named /etc/namedb	/var/named /etc/namedb
MacOS	/etc/namedb /var/named	/etc/namedb /var/named
HP-UX	/etc	/etc
AIX	/etc	/etc
OpenBSD	/etc/namedb	/etc/namedb
NetBSD	/etc/namedb	/etc/namedb
FreeBSD	/etc/namedb	/etc/namedb

How to apply and operate DNS sinkhole in Windows

Assumptions

This manual is to apply sinkhole for Windows 2000/2003 DNS server environment, and assumes as such below for friendly explanatory.

- DNS server installation directory: %SystemRoot%\system32\DNS
- Sinkhole applied zone file: sinkhole.zone
- Domain configuration file for sinkhole of malware distribution site: BOOT

✓ Please check before applying to the installation directory for bind which differs for different operating systems. (Table 1 shows common directory names for various operating systems)
✓ “sinkhole.zone”, “BOOT” files should be provided.

A. System backup and recovery

Below is explained how to backup and restore the configuration status of the DNS server, for when and after the problem occurs.

1) Backup Windows DNS configuration
   a) Stop DNS service.
   b) Backup DNS text file.
      Open the explorer, move to “%SystemRoot%\System32\DNS,” and copy the whole content of this folder to a safe location.
   c) Backup DNS registry
      Open the registry editor by run “regedit,” and move to the key below.
      “HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\DNS\Zone”
      Select “zones,” select “Export Registry File” in the file menu in the editor, and save it in the safe location.

2) Restore Windows DNS configuration
   a) Stop the DNS server service in service console in “management tool”.
   b) Open the explorer and move to “%SystemRoot%\System32\DNS”, copy the whole content of backup DNS text files.
   c) Open the registry editor.
   d) Move to the key below.
      “HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\DNS\Zone”
      Select “zones,” select “Import Registry File” in the file menu, and restore the registry.

B. Configure and apply DNS sinkhole

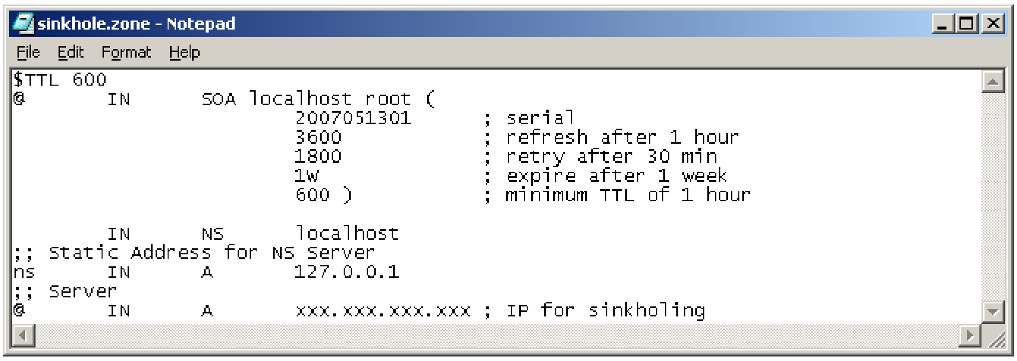
Step 1. Move to the DNS server installation directory for configuration

```
C:\> cd %SystemRoot%\system32\DNS → installation directory for name server
```

Step 2. Create the zone file for applying to sinkhole

The provided zone file “sinkhole.zone” can be copied to the directory “%SystemRoot%\system32\DNS\”.

```
c:\%SystemRoot%\system32\DNS> notepad sinkhole.zone
```



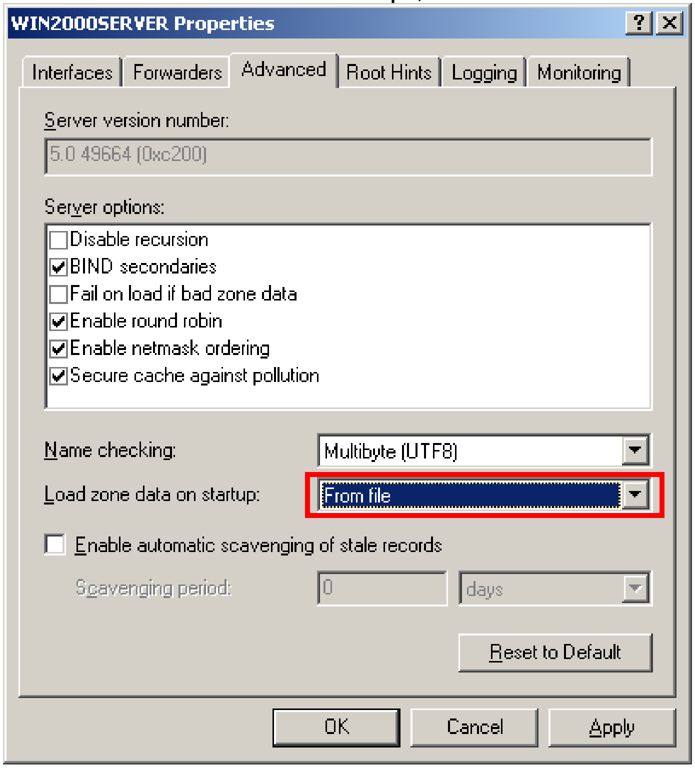
```
$TTL 600
@        IN      SOA localhost root (
                         2007051301      ; serial
                         3600            ; refresh after 1 hour
                         1800            ; retry after 30 min
                         1w              ; expire after 1 week
                         600 )           ; minimum TTL of 1 hour

         IN      NS      localhost
;; Static Address for NS Server
ns       IN      A       127.0.0.1
;; Server
@        IN      A       xxx.xxx.xxx.xxx ; IP for sinkholing
```

Step 3. Create DNS server configuration file - BOOT

If BOOT file is already used, add the content of the BOOT file provided into the existing one, otherwise, zone file “BOOT” provided can be copied to the directory “%SystemRoot%\system32\DNS\”, and applied.

✓ Change configuration for DNS server boot if newly adopted

1) Click on Start → Programs → Administrative Tools → DNS
2) Right click on the DNS in the console tree, select “Properties”.
3) Select “Advanced” Tab.
4) In the “Load zone data on startup”, select “From file”.



Server version number: 5.0 49664 (0xc200)

Server options:

- ☐ Disable recursion
- ☑ BIND secondaries
- ☐ Fail on load if bad zone data
- ☑ Enable round robin
- ☑ Enable netmask ordering
- ☑ Secure cache against pollution

Name checking: Multibyte (UTF8)

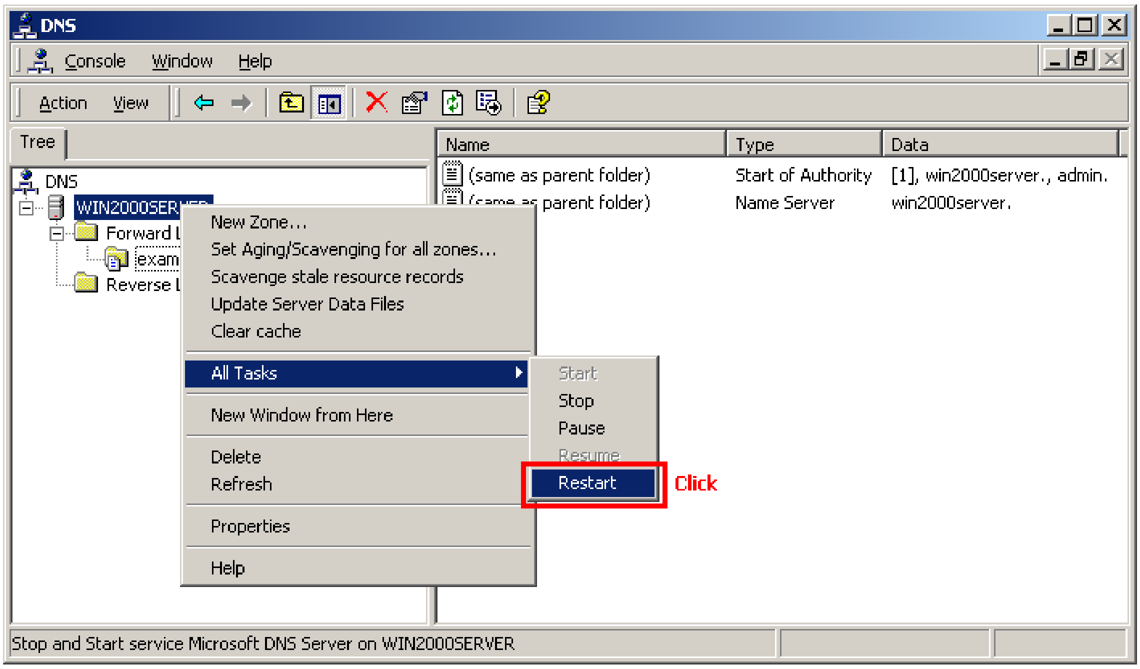
Load zone data on startup: From file

☐ Enable automatic scavenging of stale records

Scavenging period: 0 days

Step 4. Update DNS server configuration

Right click on the DNS server in the console tree, apply by selecting “All tasks”, and select “Restart.”



Name	Type	Data
(same as parent folder)	Start of Authority	[1], win2000server., admin.
(same as parent folder)	Name Server	win2000server.

Stop and Start service Microsoft DNS Server on WIN2000SERVER

☞ When BOOT file is already applied, follow through from step 3.

Appendix B

International Field Reports

- Trends and Efforts of APEC Member Economies

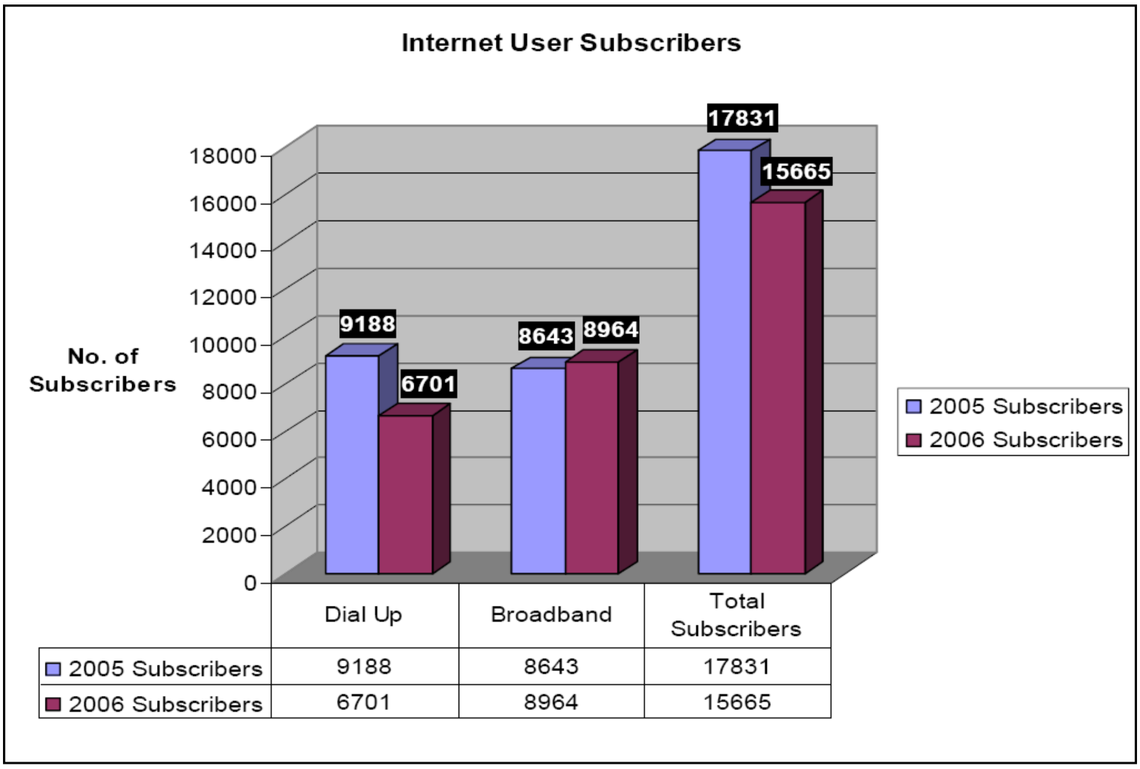
1. Brunei Darussalam

1-1. Internet Usage Statistics

<u>Internet in Brunei Darussalam</u>

Internet usage in Brunei Darussalam has been growing phenomenally since it was first launched in 1995. The 2 most popular internet connections in Brunei are the Broadband and Dial-Up technology. Based on the latest statistic (2005 and 2006) given by TelBru (BruNet) one of the ISPs in Brunei Darussalam, along with the estimated Brunei population of 380,000, there are an increased in number of users using Broadband.

The following figures provide information on the total number of subscribers using Dial-Up and Broadband Internet Connections.



	Dial Up	Broadband	Total Subscribers
▢ 2005 Subscribers	9188	8643	17831
■ 2006 Subscribers	6701	8964	15665

Figure 1

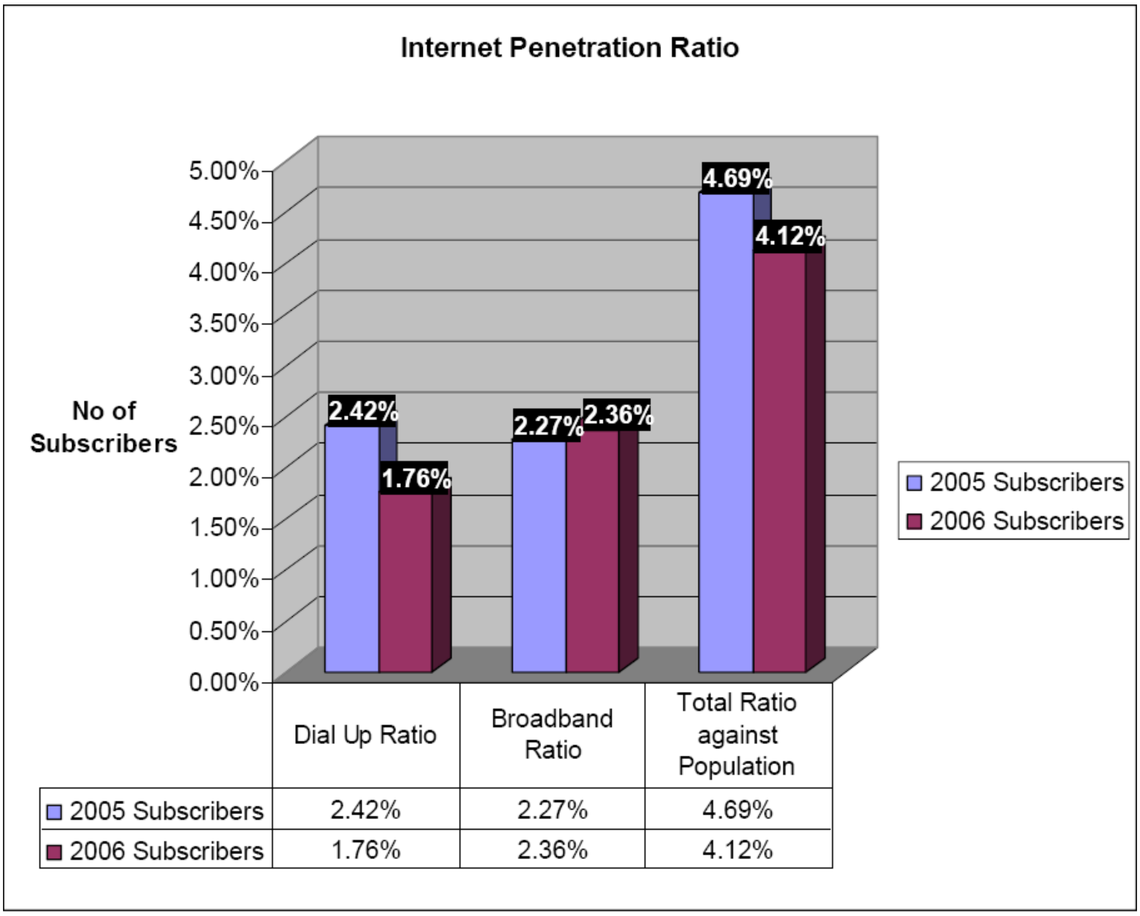


Figure 2

According to the statistics shown in both figures, it can be seen that Broadband subscribers is higher than Dial-Up subscribers from 2.27% (2005) to 2.36% (2006) and a fall in Dial-Up accounts from 2.42% (2005) to 1.76% (2006). This significant switch from dial-up to broadband usage could be influenced by the following factors:

- higher bandwidth
- provide value-added services such as onsite technical support extended broadband service coverage nationwide
- latest IT gadgets in the markets such as wireless access point
- Information, Education, Business, etc purposes

In addition from Figure 2, the total internet penetration ratio is decreasing from 4.69% to 4.12% due to the following reasons:

- a significant declined in number of dial-up users
- popularity in the use of cell-phone internet
- cybercafés which offer free internet access point with high-speed broadband internet connection

Note: Please take into consideration that this statistics did not include subscribers using prepaid cards.

1-2. National Policy and law on Information Security

Brunei Governmental Policy

Information Systems Security Policy
The purpose of this policy is to provide a comprehensive set of general guidelines for the responsible and secure use of the ministries or departments information flow and the resources. In addition to the human aspect of the security program, technical solutions continue to be implemented for both the perimeter and internal host protections. The overall strategy of ministry or department Information Security Policy is to protect all critical information assets against internal and external threats via the effective implementation of the policy. This Information System Security addresses technical, physical and administrative domains, as they might affect the security of information.

Laws of Brunei

i. Electronic Transactions Order, 2000

The **Electronic Transactions Order, 2000** was recommended to be introduced mainly to address the issues pertaining to the conduct of online business transactions. The main objectives of this Order among others include enabling and facilitating the use of electronics signatures and providing equal treatment to users of paper based documentation and users of computer based electronic documentation. It is intended that this legislation can spearhead Brunei to foster the delivery of both public and private sector services online. The ETO was specifically made to ensure that an electronic transaction shall not be treated as legally invalid simply because it was made electronically.

ii. Brunei Computer Misuse Order 2000

The Computer Misuse Order, 2000 (CMO) complements the ETO, in that it raises confidence in Brunei Darussalam by providing for a variety of offences against computers. There are enhanced punishments for offences against *protected computers*.

Unauthorised access to computer material.
In general, if found guilty, liable on conviction to a fine not exceeding five thousand dollars, imprisonment for a term not exceeding two years or both.

Access with intent to commit or facilitate commission of offence.
In general, any person guilty of an offence under this section is liable on conviction to a fine not exceeding fifty thousand dollars, imprisonment for a term not exceeding ten years or both.

Unauthorised modification of computer material.
In general, any person guilty of an offence and is liable on conviction to a fine not exceeding ten thousand dollars, imprisonment for a term not exceeding three years or both.

Unauthorised use or interception of computer service.

In general, any person is guilty of an offence and is liable on conviction to a fine not exceeding ten thousand dollars, imprisonment for a term not exceeding three years or both.

Unauthorised obstruction of use of computer.
In general, any person guilty of an offence and liable on conviction to a fine not exceeding ten thousand dollars, imprisonment for a term not exceeding three years or both.

Unauthorised disclosure of access code.
In general, any person guilty of an offence and is liable on conviction to a fine not exceeding ten thousand dollars, imprisonment for a term not exceeding three years or both.

Enhanced punishment for offences involving protected computers.
In general, the person convicted of such offence is in lieu of the punishments respectively prescribed in those sections, liable on conviction to a fine not exceeding one hundred thousand dollars, imprisonment for a term not exceeding twenty years or both.

iii. **Aiti Order 2001**
The **AiTi Order, 2001** establishes the Authority for Info-communications Technology Industry of Brunei Darussalam (AiTi) as an independent statutory body to regulate the local ICT industry, and provides for its functions and duties. This Order was brought into effect on 1st January 2003.

iv. **Telecommunication Orders 2001**
The **Telecommunications Order, 2001** confers upon AiTi the exclusive privilege to operate and provide telecommunication systems and services in Brunei Darussalam and allows AiTi to grant of licenses for the same. Once this Order is brought into force, AiTi will enforce its licensing power and functions as outlined in the AiTi Order 2001.

v. **Broadcasting Act 200**
The **Broadcasting Act, 2000** regulates dealing in, the operation of and ownership in broadcasting services and broadcasting apparatus, and for connected purposes.

1-3. CERT Services and Statistics on Malicious Activities

About BruCERT

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

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.

BruCERT Activities in 2007

Attended Seminars/Conferences/Meetings/Visits

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

- In March 28th – 29th 2006, three representatives from BruCERT had attended the 5th APCERT Conference held in Beijing, China.
- In July 28th 2006, BruCERT join the ASEAN CERT incident Response Drill, where the main focused is to test the communication within the CERTs from different ASEAN countries.
- On the 18th till 22nd September 2006, two (2) representatives from BruCERT attended the 2006 APEC Security Training Course in the Republic of Korea.
- In December 19th 2006, BruCERT with 15 other teams from THE 13 regional economies participated in the APCERT annual drill, to test the timeliness and response from other CERT and CSIRT throughout the region.
- In 8th February 2007 - Two BruCERT delegates attended the APCERT 2007 Annual General Meeting which takes place at Langkawi, Malaysia.
- On the 22nd till 27th May 2007, BruCERT participated in Civil Service Institute Customer Day held at Civil Service Institute in the capital.
- In July 16th 2007, BruCERT join 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 Aug 2nd 2007, three of JPCERT delegates lead by its Director of Technical Operation paid a courtesy visit to BruCERT premise.

Training and Seminars

From January 2007 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.

Due to overwhelming response, the “Basic Information Security Workshop” was developed in May 2007 as an advanced course from the IT Security Awareness training. This particular training will be conducted on a regular basis at the Civil Service Institute, Brunei.

BruCERT Future Plans

- Applying for FIRST membership
  BruCERT plans to upgrade its member status to full member in APCERT and work on with other terms and conditions to qualify for the FIRST membership.

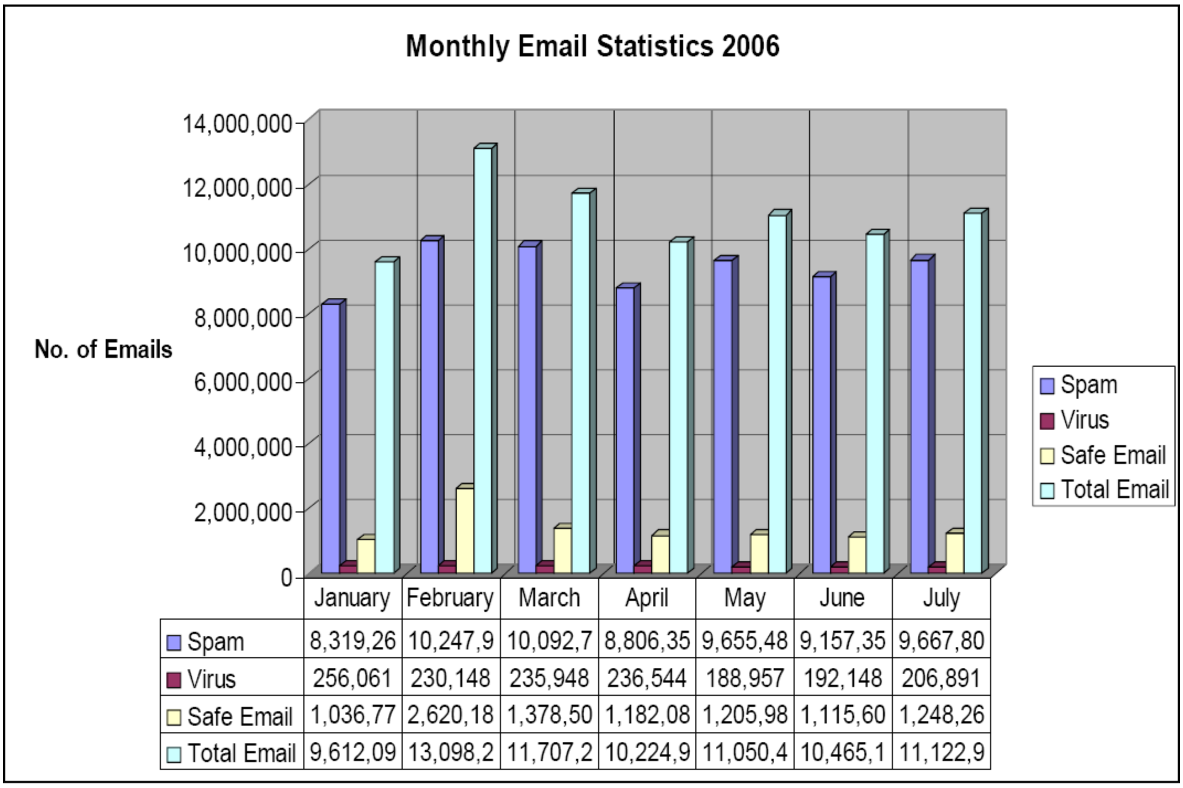
- Free Seminars to the local public
  A half-day or one-day talk will be given to the local public to enhance awareness on IT security-related topics.

- SMS Services
  BruCERT plans to offer SMS alert and notification service for the public. This subscription based service shall provide early notification to the public on IT security related events and alerts.

- BruCERT Road shows
  Organize Roadshows to further promote and publicize BruCERT services by conducting, educational programmes and games.

- Publications
  Produce educational booklets and posters. This is intended to provide basic IT security awareness to the general public and facilitate BruCERT road shows.

<u>Statistics on malicious codes</u>



	January	February	March	April	May	June	July
■ Spam	8,319,26	10,247,9	10,092,7	8,806,35	9,655,48	9,157,35	9,667,80
■ Virus	256,061	230,148	235,948	236,544	188,957	192,148	206,891
□ Safe Email	1,036,77	2,620,18	1,378,50	1,182,08	1,205,98	1,115,60	1,248,26
□ Total Email	9,612,09	13,098,2	11,707,2	10,224,9	11,050,4	10,465,1	11,122,9

Figure 3

As shown in Figure 3, spam is more popular than viruses. This might be because of the ISP had implemented an additional new hardware to assist in detecting spam mails as well as viruses and furthermore that the advantage of free advertisement through email seems to be at ease. While during February, the high percentage email utilization could possibly due to no new big impact viruses ever exist during that period.

As BruNet still lack of complete logging mechanism necessary for more effective and complete monitoring, thus they only managed to gather the statistics above. But they are in the process of upgrading their capabilities through their own initiatives or through some corroborative work with BruCERT.

1-4. Information on Constituency

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

1. <u>Government Agencies</u>
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.

2. 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.

3. Royal Brunei Police Force

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

4. TelBru – BruNet

The main service provider of internet gateway. BruCERT and TElBru have been working together to engage information sharing of internet-related statistics and the current situation of IT environment in Brunei.

5. DST

The second largest internet service provider in Brunei.

6. DELL

Being appointed as a System Integrator (SI) and Distributor for Dell products and services in Brunei.

7. INGRAM MICRO

As a strategic partner in providing TrendMicro (Antivirus), various computer products and services to the Brunei market.

8. EC-Council

ITPSS has become a training partner for EC-Council which offers IT Security and E-Business solutions, trainings and certifications.

9. JPCERT/CC

Having close relationship and cooperation between both BruCERT and JPCERT to gain further understandings in IT related environment for both countries.

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.

2. China

2-1. Internet Usage Statistics

- Internet Penetration ratio and broadband subscribers in China
By June 2007, the total of Internet users in China had reached 162 million (Fig.1), only next to the 211 million3 of United States, ranking the second in the world. Twenty-five million are newly increased as compared with the total number at the end of 2006, and 39 million within a year as compared with that in the same period of 2006. The growth rate was up to 31.7%, entering a new round of rapid growth.

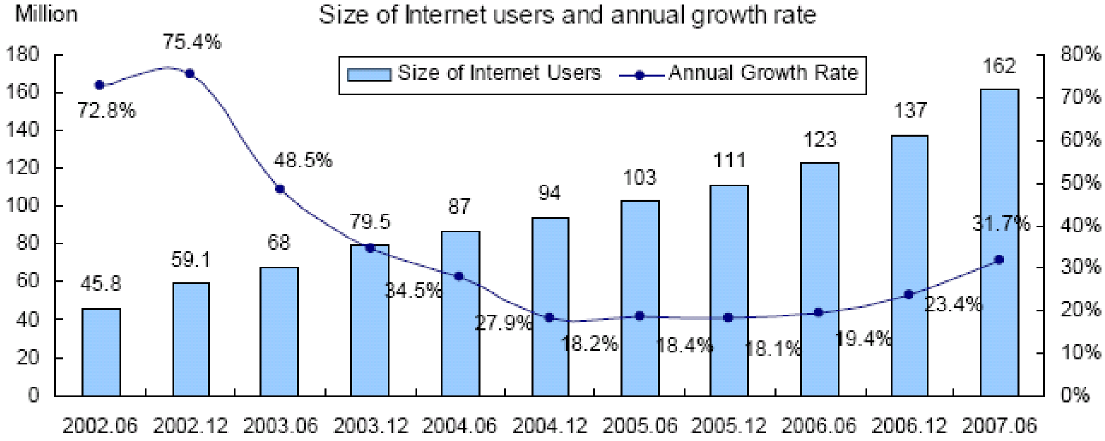


Fig.1 The size and annual growth rates of Internet users in China

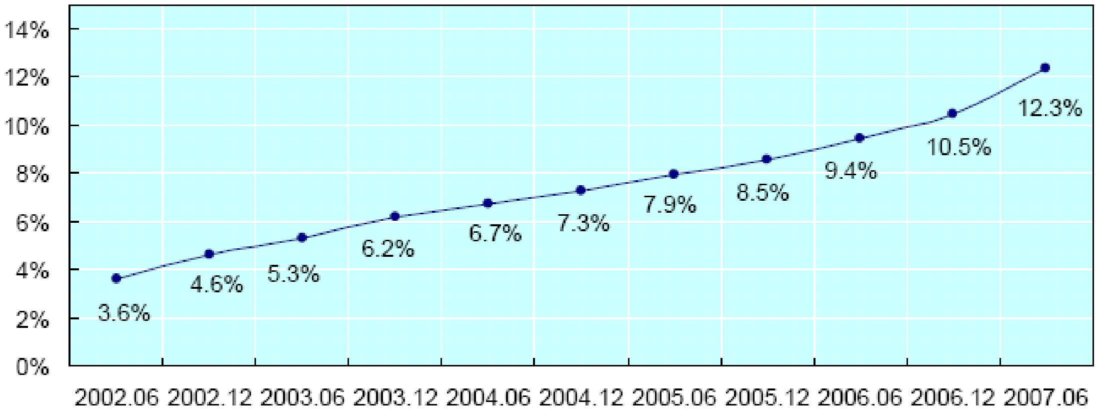


Fig.2 Internet penetration rate in China

The Internet penetration rate in China reaches 12.3% at present, increasing about 3 percentage points compared with 9.4% in the same period of 2006 (Fig. 2). Internet is increasingly widely used in China; more and more people will have access to and benefit from it. According to the statistics by the CNNIC, 99% of those accessed the Internet would continue to access the Internet.

Of the total 162 million Internet users, broadband (including dedicated lines) users have already been up to 122 million. The increase in broadband users implies that the access conditions in China have been further improved and therefore more users could enjoy pleasant visits to the Internet with faster speed and more stable connection. The ADSL and dedicated line account for a considerable proportion of the broadband users.

The trend of development and the amount of Internet users vary across the main access methods. Compared with that of the end of December 2006, the amount of broadband users (including dedicated line) obviously went up, with an increase of 18 million within half a year. In particular, the number of dedicated line users grew steadily to 28.80 million, by a slight increase of 1.7 million; the number of dial-up users continues to decline, and nevertheless more than 31.60 million users are dial-up users.

Wireless access, especially the mobile phone Internet access has developed rapidly in China. Satisfying some users' special needs, it has a certain size of users. The wireless users add up to 55.64 million at present (Fig. 3), and in particular the size of mobile phone users is 44.30 million.

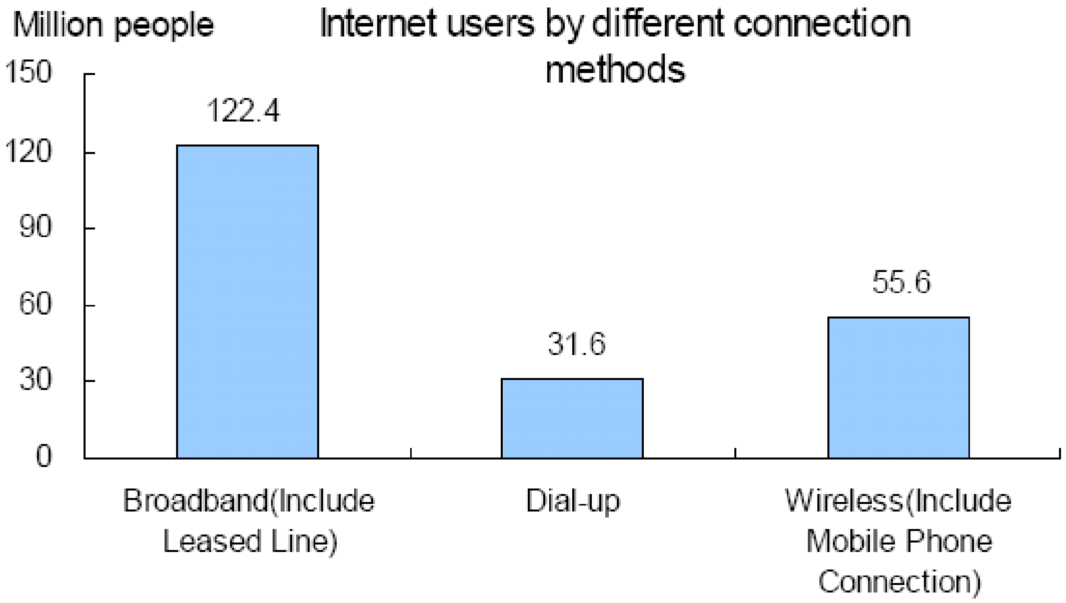


Fig.3 Size of Chinese Internet users by access method

- Major Internet Service Providers in China
There are four Nation-wide Internet Service Providers in China

- CERNET: China Education and Research Network
- CSTNET: China Science and Technology Network
- CHINANET: China Public Computer Internet
- GBNNET: Golden Bridge Information Network

2-2. National Policy and law on Information Security

1. Interim Regulations Governing the Management of International Computer Networks
2. Computer Information Network and Internet Security, Protection and Management Regulations

3. Management Measures of the People’s Republic of China Regulations for the Safety Protection of Computer Information Systems
4. State Secrecy Protection Regulations For Computer Information Systems on the Internet
5. Computer Information System Security Protection Ordinance of People’s Republic of China
6. Criminal Law of People’s Republic of China
7. Rules of Computer Virus Protection and Disinfections Management

2-3. CERT Services and Statistics on malicious activities

1. In 2006, CNCERT/CC received 26476 incident reports from domestic and oversea sources, exclusive scan incidents.
2. In 2006, CNCERT/CC published 87 vulnerability advisories, which are all about main stream OS and applications, and considered to be highly dangerous.
3. In 2006, CNCERT/CC detected more than 16k oversea C&C servers that controlled the Botnet in China.
4. In 2006, CNCERT/CC detected about 28070 defaced websites in mainland China.Of the total number, the government sites (with .gov.cn domains) make up 13.6%, showing the poor security condition of government websites.

2-4. Information on Constituency

1. CNCERT/CC delivered many information security reports to government departments, ISPs, key information infrastructures and the public.
2. Meanwhile, CNCERT/CC conducted information and data sharing with trusted oversea partners.
3. The range of objects and partners to provide information has been prudently extended and the number has been increased.
4. The information was delivered in form of special report, email and website bulletin.
5. Hosted the APCERT’2006 AGM and CNCERT/CC’2006 Conference jointly at Beijing in March, 2006.
6. Hosted China-ASEAN Internet Security Emergency Response Seminar at Beijing in Dec. About 20 delegates from CERTs and governments of ASEAN countries attended the seminar.
7. As the deputy Chair, on behalf of APCERT, addressed on the 34th APEC TEL plenary, and gave presentations for the slot of APCERT on the 35th APEC TEL.
8. Sponsored AhnLab of Korea and CMCERT/CC of China to join FIRST.
9. Attended the FIRST-TC in Sep and delivered a technical report.
10. Co-planned and joined the APCERT IH Drill’2006.

3. Hong Kong, China

3-1. Internet Usage Statistics

In Hong Kong, Internet is a very popular tool for both business and household sectors. In the August 2005 Hong Kong Special Administrative Region (HKSAR) Government report of “Penetration of Information Technology in the Household Sector,” 70.1% households in Hong Kong have personal computers, and 64.6% households with personal computers at home are connected to the Internet. As of September 2004, the figure issued by Hong Kong Office of the Telecommunications Authority (OFTA) showed that broadband Internet customer accounts exceeded 1.4 million while the household broadband penetration rate was very close to 59%.

Internet Service Providers (ISPs) in Hong Kong are operated by commercial entities. They are regulated by the OFTA rules. HKSARG Government and the Hong Kong Police Force (HKPF) do not interfere the daily operations of ISPs. In crime investigation, HKPF would obtain court order to command ISPs to release information or evidence. In case of any Internet attack, ISPs follow their operation procedure to take action. ISPs do not have the same operation procedure to handle virus attack, hacking attack and spam mail. Their response level varies. For health monitoring, ISPs monitor the major international connections, the IP level network bandwidth utilization and packet rate abnormality. They have a general abuse contact to handle security incidents.

HKCERT handles many incident reports on phishing, virus and hacker attacks. We also monitor the defaced web sites with “.hk” domain reported by the Zone-H portal. We handle the problem by sending email or phone call to the victim or their ISPs. When the incident involves crime, we will also forward a report to HKPF. When HKCERT receives critical report about massive attack or virus out-break, we contact the HKSAR Government, HKPF and the ISPs to take appropriate action. HKCERT also issue press release to the media. The hype in using media was in years 2003 and 2004 for SQL Slammer, Blaster, Welchia and Sasser worms.

3-2. National Policy and Law on Information Security

HKSAR Government computer system security is managed by the government department “Office of the Government Chief Information Officer (OGCIO).” This department also provides education and awareness promotion on computer security. HKPF deals with law enforcement and investigation issues. Within HKPF, the cyber crime issues are delegated to the Technology Crime Division of the Commercial Crime Bureau. HKCERT provides a central coordination point for information security matters. We provide the free hotline and email service to general public on security incidents and enquiry. HKCERT, HKPF and OGCIO formed a standing closed group called CONNECT to continuously communicate on information security issues. CONNECT is a key channel for cyber security watch in the World Trade Organization Ministerial Conference held in 2005 in Hong Kong. HKCERT also keep on passing updated technical or vulnerability information to CONNECT. HKCERT also worked closely with HKPF in handling phishing and botnet cases. Since HKPF has a close tie with the Hong Kong Monetary Association and the Hong Kong Association of Banks, HKCERT can indirectly communicate with the financial industry. HKCERT frequently collaborate with HKPF in giving security updates to the financial industry. CONNECT is a platform for HKCERT, HKPF and OGCIO to collaborate in security awareness promotion to the general public like the Clean PC Day campaign. In Hong Kong there is not a dedicated law for computer crime. The current computer crimes ordinance was enacted in 1993 through amending the Telecommunications Ordinance (Cap. 106), Crimes Ordinance (Cap. 200) and Theft Ordinance (Cap. 210) to create some new offences and broadening the coverage of existing offences. The maximum penalty is 14 years' imprisonment or fine of $20,000 Hong Kong dollars.

3-3. CERT Services and Statistics on malicious activities

HKCERT is the recognized representative CERT for the economy of Hong Kong. The main objective of HKCERT is to help the general public and small and medium enterprise to resolve computer security problem. HKCERT also handles cross-border security incidents. We receive overseas report on phishing site, virus and hacker attack sourced from Hong Kong. We contact HKPF and ISPs to close down the sources of attack. HKCERT received the highest number of incident reports in 2003 and 2004 with a majority of virus incidents. As the hacker motivation changes from personal satisfaction to monetary benefits, the attacks are stealthier. The number of incident reports is dropping. However the complexity of the incidents is higher and the involvement with overseas coordination is increasing. In the long run, HKCERT plan to build an Internet Security Threat Monitoring and Early Warning System. We are planning a feasibility study on it this year.

3-4. Information on Constituency

HKCERT serves the general public and small and medium enterprises (SME). They are in general lack of resources and knowledge to deal with cyber attacks. In Hong Kong, security seminars provided by vendors are abundant. People can access to product information with no problem. From HKCERT survey in 2001-2004, the adoption of antivirus and firewall technologies are growth satisfactorily. However, the community is still weak in security management, backup management and patch management. HKCERT has also been actively working with education sectors in promoting security in schools. HKCERT has started a project to enhance the communication with ISPs to speed up the handling of security incidents and let them better use the HKCERT resources to resources from international CERT to close down sources of attack from overseas.

4. Malaysia

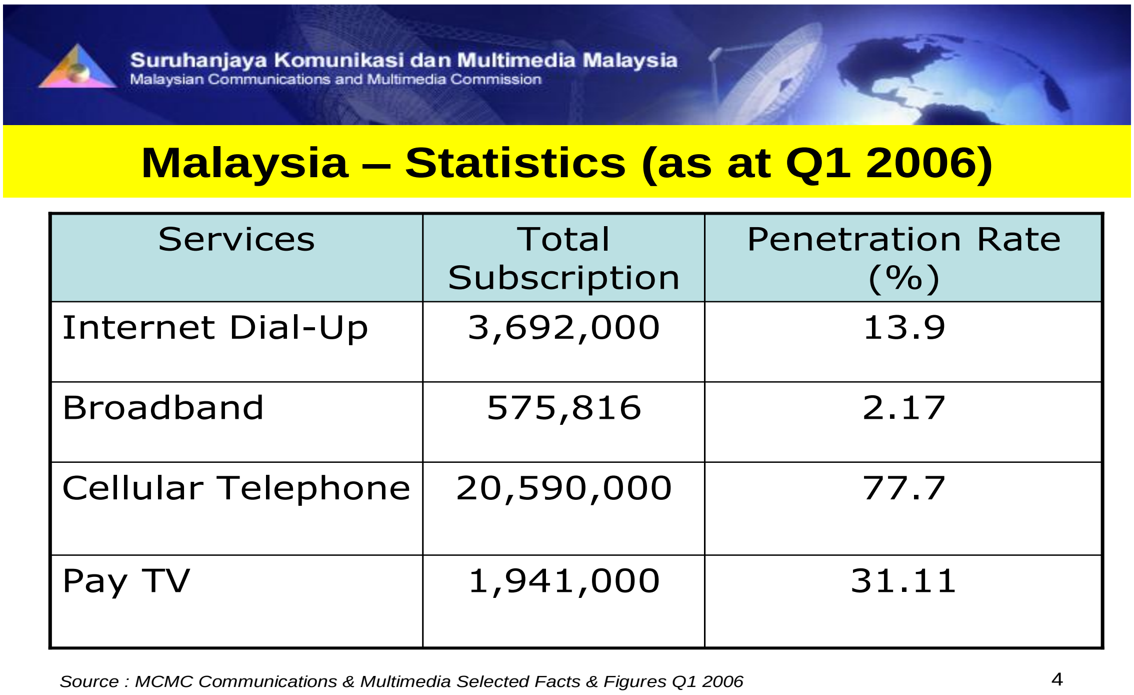
4-1. Internet Usage Statistics

(a) Internet Penetration

Internet Penetration Ratio is about 13.9% (3.6 million users) as at Q1 of 2006. Forecast for Q4 of 2006 is 14.3% (3.8 million users). Target for Q4 of 2007 is an increase to 30 % (7 million users).

(b) Broadband penetration

Broadband penetration is 2.17% (540,000 users) as at Q1 of 2006. In Q2 of 2006 the figure has increased to 2.5% (650,000 users). Target for Q4 of 2006 is an increase to 5% (1.3 million users).



Suruhanjaya Komunikasi dan Multimedia Malaysia
Malaysian Communications and Multimedia Commission

Malaysia – Statistics (as at Q1 2006)

Services	Total Subscription	Penetration Rate (%)
Internet Dial-Up	3,692,000	13.9
Broadband	575,816	2.17
Cellular Telephone	20,590,000	77.7
Pay TV	1,941,000	31.11

Source : MCMC Communications & Multimedia Selected Facts & Figures Q1 2006

4

(c) Major Internet Service Providers

There are 7 major IASPs namely, TMNet, JARING, TIMENet, Celcom, Maxis, DiGi and NTT MSC. Other players include Airzed, Arcnet, Atlas One, Bizsurf, Nasioncom etc.

As at Q1 of 2006 Malaysia had a total of 414 Applications Service Provider (ASP) Class Licensees. A holder of ASP Class License is allowed to provide audiotext hosting services on an opt-in basis, directory services, **Internet access services**, messaging services etc.

(d) Relationship with ISPs

(i) Information Sharing Forum (ISF)

MCMC has set up the Information Sharing Forum (ISF) in April of 2004 with the objective to bring together relevant parties into a single forum to share their experiences and expertise for the benefit of the Malaysian network infrastructure and to establish an effective information sharing mechanism.

The ISF comprises of MCMC, together with the ICT Security Division of MAMPU, the National ICT Security Emergency Response Centre (NISER), Malaysian Technical Standards Forum Berhad and various Internet Service Provides (ISPs).

This coordination effort is to enable different network operators, internet backbone providers and other interest groups to analyze and exchange data about attacks and in order stop exploits from escalating and causing damage or disruption of vital systems.

Such exchange of information is hoped would improve analysis, warning, response and recovery with long-term benefits for the public and private sectors. Further it would help minimize damages from online security attacks with the implementation of faster incident handling, preventive and corrective action.

(ii) Internet Access Service Provider (IASP) Sub-Code

Under the self regulatory framework of the CMA, the industry fora develop codes and promote compliance among industry members. There are four such fora each in the area of access, consumer protection, technical standards and Content. One such forum is the Communications and Multimedia Consumer Forum of Malaysia (CfM).

CfM is a body designated under the CMA and has been given the responsibility to develop codes and sub-codes for dealing with matters relating to the protection and promotion of consumer interests in relation to specific services including, but not limited to, the matters listed in the CMA.

The General Consumer Code of Practice (GCC) has been registered in October 2003. The IASP Sub-code aims to supplement this GCC code in the area of Internet access services provisioning. It was registered on 1 June 2005 and is administered by the CfM. (www.cfm.org.my)

The IASP Sub-code provides general rules on service provisioning for Internet Service Providers. Among others, it addresses anti-SPAM measures, protection of personal information, protection of minors, and policy on information network security and handling of customer complaints and disputes.

4-2. National Policy and Law on Information Security

The Law and Policy

(a) Communications and Multimedia Act 1998

MCMC is a statutory body established under the Malaysia Communications and Multimedia Commission Act 1998 to regulate and nurture the communications and multimedia industry in Malaysia in accordance with the national policy objectives set out in the Communications and Multimedia Act 1998 (CMA).

The MCMC is also charged with overseeing the new regulatory framework for the converging industries of telecommunications, broadcast and online activities. The 10th National Policy Objective, as stated in the CMA requires the Commission to ensure information security and the integrity and reliability of the network for the country.

Legal issues relating to network security are addressed in the CMA and the Computer Crimes Act 1998. Under the CMA (Section 3(2)(j)), the Commission is entrusted to ensure information security and the reliability and integrity of the network. For example, fraudulent use of network, improper use of network facilities/services and interception of communications are addressed in the CMA.

(b) Computer Crimes Act 1998

Under the Computer Crimes Act, acts such as unauthorized access to computer material and with intent to commit or facilitate commission of further offence, unauthorized modification of contents of any computer and wrongful communication is addressed.

(c) National Information Security Policy (NISP)

Currently a study is underway to develop the National Information Security Policy. The objective of this study is to access the current situation of information security in various critical sectors in Malaysia and chart a Roadmap and Action Plan to develop (NISP).

Under the said study a total of ten sectors have been identified as representing the Critical National Information Infrastructure (CNII) being, National Defense & Security, Banking & Finance, Information & Communications, Energy, Transportation, Water, Health Services, Government, Emergency Services – e.g., Fire and Rescue Services and Food & Agriculture. A National Coordinating Centre will also be set up to coordinate the national information security initiatives.

(d) Communications and Multimedia Information and Network Security Policy

MCMC is currently developing a policy paper on Information Network Security It encompasses six main areas of priority/aims/goals involving the relevant stakeholders and to some extent, parties representing other critical infrastructures which includes securing the industry, promoting awareness, capacity building, information sharing and international cooperation.

(e) Agencies Involved

In Malaysia, various bodies have been formed for the purpose of promoting or ensuring information network security.

Some of these include:

a. MAMPU's (Malaysian Administrative Modernization and Management Planning Unit) ICT Security Division

   MAMPU's ICT Security Division has the responsibility of ensuring ICT security matters for the public sector. This is done through the Malaysian Public Sector Management of Information and Communications Technology Security Handbook.

   The handbook provides the necessary guidelines on ICT security management safeguards to enable implementation of minimal security measures. It discusses elements of management safeguards, common operational and technical issues, and legal implications.

   The ICT security management safeguard identify five (5) major elements that should be considered by all public sector ministries, departments and agencies to protect their ICT systems. The elements are ICT security policy, ICT security management programme, ICT security risk management, planning and incorporation of ICT security into the ICT systems' life cycle and establishing ICT security assurance.

b. National ICT Security and Emergency Response Centre (NISER)

   NISER was set up under the auspices of the National Information Technology Council (NITC). NISER is tasked with the following:-

   i) Conducting vital technical and remedial action at sites affected by security incidents.
   ii) Providing services to both the public and private sectors which include incident response, security inquiry services, technology research and assessment, expert services, acculturation programme and community services.

c. ICT Security Standard Working Group

   The ICT Security Standard Working Group comprising several representatives from various organizations in the public and private sector that meet, deliberate and decide on the adoption of all security standards in Malaysia. These standards are mainly those that are ISO status standards where the Working Group will use their expertise to deliberate and adopt the relevant security standards as a Malaysian Standards (MS).

d. Information Network Security Department (INS) in MCMC

Some of the work undertaken by INS:-

(i) Setting up of the ISF and coordinating the same;
(ii) Yearly security audits to assist in identifying weaknesses within the licensees' networks and provide suggestions on how these vulnerabilities should be protected.
(iii) Awareness program on spam
(iv) Workshops and industry talks on INS especially on incident handling response.
(v) Midst of setting up the Network Monitoring Centre and Abuse Reporting Portal which will provide the following:-

- ❖ Threat Monitoring and Early Warning;
- ❖ Vulnerability Management; and
- ❖ Incident Management and Forensics

4-3. CERT Services and Statistics on malicious activities

(a) CERT Services

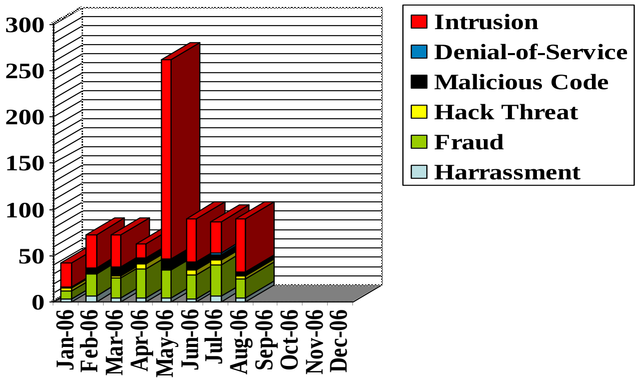
The Malaysian Computer Emergency Response Team (MyCERT) was formed on January 13, 1997 and started its operation fully on March 01, 1997.

Its mission is to address the computer security concerns of local Internet users and to provide a point of reference for the Internet community here to deal with computer security incidents and methods of prevention.
Some of the functions of MyCert are as follows:

- ❖ Provide a point of reference of expertise on network and security matters
- ❖ Centralizes reporting of security incidents and facilitates communications to resolve security incidents
- ❖ Disseminate security information including system vulnerabilities, defence strategies and mechanism
- ❖ Act as a repository of security related information, acquiring patches, tools and techniques
- ❖ Plays an educational role in educating the public with regard to computer security in Malaysia

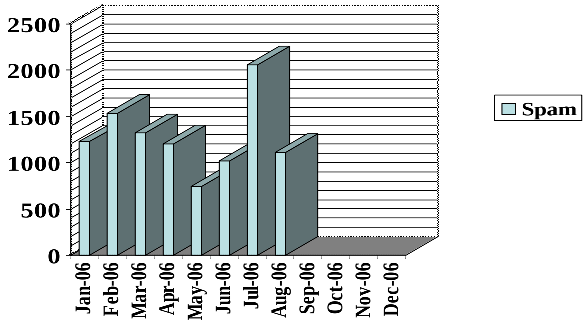
(b) Selected Statistics

Incident Statistics
(August 2006)



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Harassment	3	7	4	4	4	3	6	4				
Fraud	9	23	22	32	31	26	34	21				
Hack Threat	3	1	2	5	0	6	5	3				
Malicious Code	1	6	10	7	12	8	6	5				
Denial of Service	0	0	0	0	0	2	0					
Intrusion	26	36	35	15	215	47	34	56				
TOTAL	42	73	73	63	262	90	87	90				

Spam Incident Statistics
(August 2006)



Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Spam	1227	1538	1323	1200	743	1021	2059	1115			

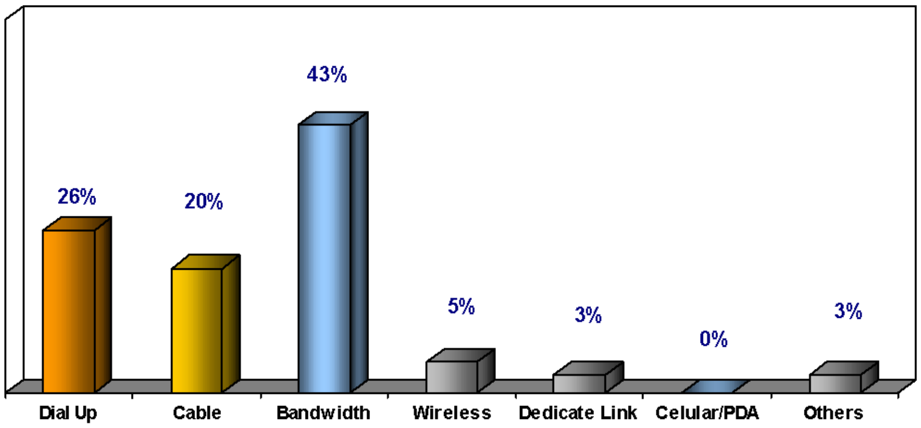
5. Mexico

5-1. Internet Usage Statistics

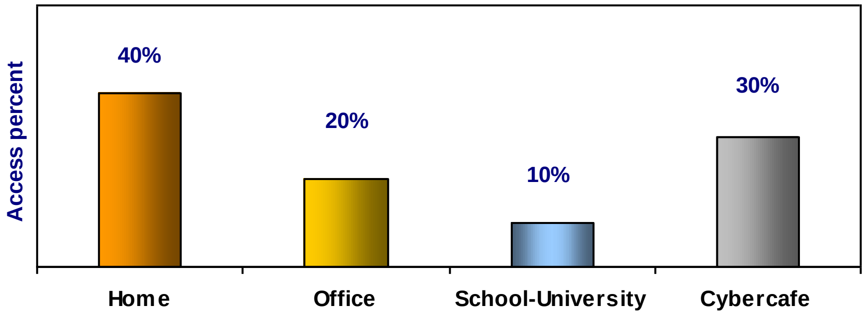
The statistics of the Internet use in Mexico are showing a major use of this technology in electronic commerce, transborder data flow, and interchange of sensitive information. For theses reasons is necessary to have security mechanisms and a legal system that allow the immediate response to incidents of information security.

In Mexico the amount of PC is distributed as follows: 42 % in office and 58 % in homes. There are 3.5 millions users and the type of connection is: 1.8 million Dial-Up, 1.7 bandwidth and 12 thousand of dedicated link.

Type of Internet Connection



More frecuent access



- Major Internet Service Providers in your economy

In Mexico there are more than 1000 providers of IPS's and NSP's but the majority of the personal accesses use the main providers companies like: TELMEX, ATT, TV cable.

The relation between the different providers of Internet service is given through Mexico NIC Nevertheless it does not exist national regulations to determine which the minimal level of security is.

The information security is given in function to the company prestige. It is very important to have contracts services in order to assure the service level according with the users needs.

5-2. National Policy and law on Information Security

Mexico is doing several efforts in the computer legislation area that allow actuating in an efficient way against incidents of technological security. This legislation has to look for the users' privacy right but at the same time to allow the government has access to tracking incidents.

Federal Administration Institutions related with the computer activities
Secretaría de Gobernación

- Secretaría de Relaciones Exteriores
- Secretaría de Hacienda y Crédito Público
- Secretaría de Economía
- Secretaría de Comunicaciones y Transportes
- Secretaría de Contraloría y Desarrollo Administrativo
- Secretaría de Educación Pública
- Comisión Federal de Telecomunicaciones
- Consejo Nacional de Ciencia y Tecnología

Legislation related with the computer activities

- Copyright Law
- Industrial Property Law
- Federal Telecommunications Law
- Statistical and Geographical Information Law
- National Security Law

Juridical initiatives in computer matter.

- Computer crimes, March 22/2000
- E-mail (April 29/1999; December 15/1999; March 22/2000)

In Mexico there are computer aspects contemplated in the current legislation:

- Copyright and industrial property.
- Patents, commercial names, industrial secrets.
- Communications regulation

The following aspects are not contemplated in the legislation

- Computer crime tipification

- Illicit use of computer equipment
- Juridical Security in the use of electronic jeans

Others aspects that have been promoted to be included in the legislation are:

- Minors' protection and promotion to the protection of confidential information;
- Legal aspects related with the use of e-mail.
- Confidentiality of the information
- Intimacy persons protection
- Validity of electronic documents

5-3. CERT Services and Statistics on malicious activities

In Mexico important steps has been taken in order to have an organization similar to a CERT. In this effort are involved government institutions,, companies, civil associations and universities..

At this moment we have a federal cybernetic policy. Some universities has their own CERT but they are limited to academic areas. Mexico needs to work in the organization of a National CERT located in one of the National Security Agency.

Surveys related to the information security reveal the importance to create a CERT.

- Scarcely 3.8 % of the companies counts or knows of political and basic procedures for the information security.

- 67 % of the users write in paper his passwords and 67 % never changes them.

- The half of the attack to a system they come from the interior of the organization and another half of the exterior.

- The companies spend between 12 and 18 per cent of his income in technology; of this percentage, the expense in security occupies between five and eight per cent.

- 81.8 % of the people use personal computers in the home and the office and the rest only in the office.

- The viruses continue being the principal threat for 87.9 % of the interviewed ones.

- 10.9 % of the polled ones meditate as risk to the wireless systems.

- 31.3 % of the interviewed ones consider the application of antivirus to be a principal measurement against the insecurity; 27 % the training; and 25.7 % the suitable managing of passwords.

6. New Zealand

6-1. Internet Usage Statistics

Background

New Zealand Population: 4,195,730 million (2006 Estimate)

The following provides information on the total number and nature of subscribers who use New Zealand-based Internet Service Providers (ISPs) to connect either continuously or regularly to the Internet.

Highlights

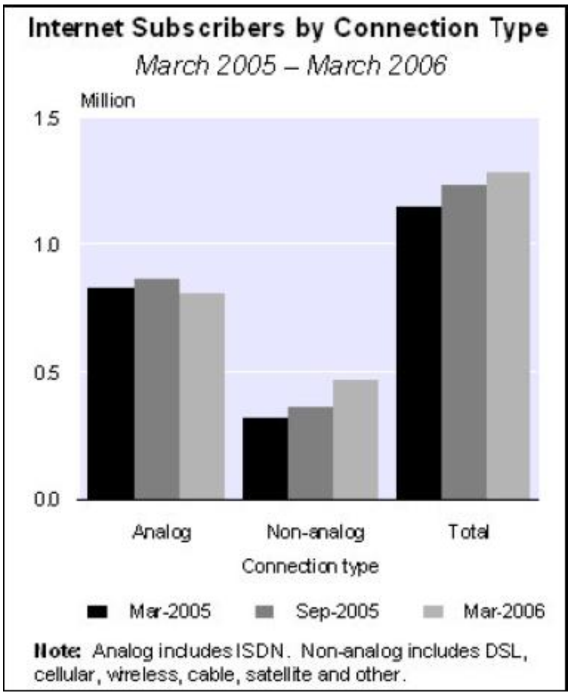
In the six months ended 31 March 2006

- **There were 57 Internet service providers (ISPs) in New Zealand**, with 1.29 million active subscribers.
- **Analog was the predominant connection technology**, with 812,300 active subscribers.
- **The number of non-analog subscribers increased 29 percent** from 30 September 2005, to 475,700.
- **There were 31.2 active Internet subscribers per 100 inhabitants**, up from 28.2 per 100 at 31 March 2005.
- The predominant download speed category was less than 64kbps.
- 79% of ISPs in New Zealand saw the strength of competition as the greatest barrier to growth of their operations.

Internet Subscriber Connection Type

The number of subscribers using analog connection technology (also known as dial-up) decreased 6.6% from 30 September 2005, to 812,300 subscribers. Analog is still the most used connection technology, with 63% of total subscribers at 31 March 2006, down from 70% of subscribers at 30 September 2005.

Non-analog subscribers (also known as broadband subscribers) jumped 29% from 30 September 2005, to 475,700 subscribers. Of the non-analog connections, Digital Subscriber Line (DSL) continues to be the most common connection technology. The ranking of the next most common non-analog connection technologies in descending order was: cellular, wireless connections, cable, satellite, and other. The ranking is the unchanged from 30 September 2005.

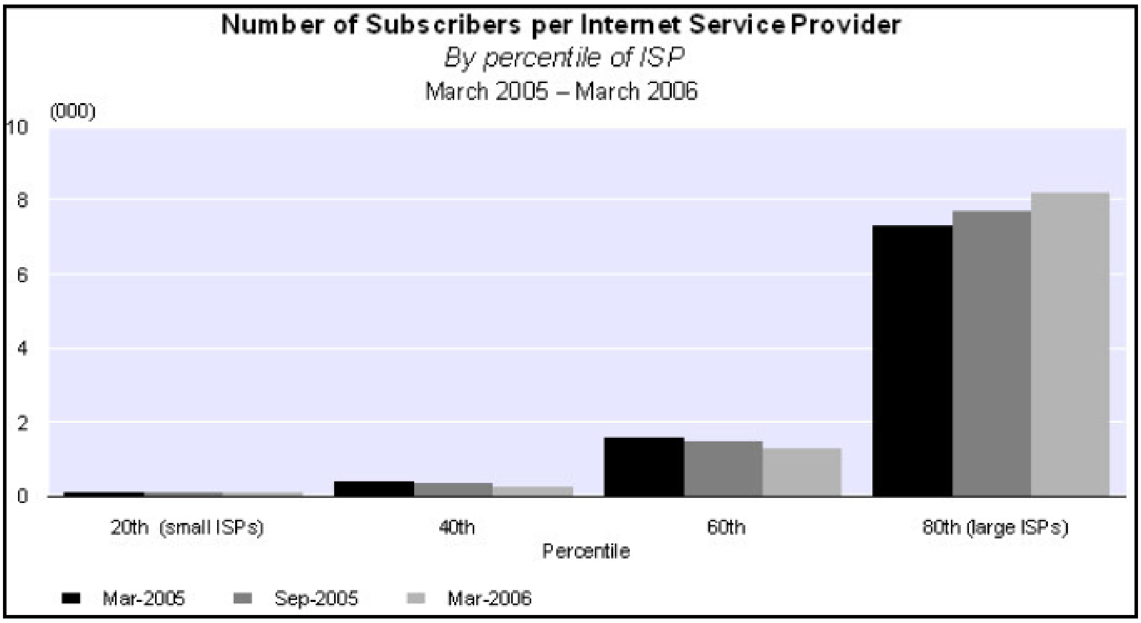


There were 31.2 Internet subscribers per 100 inhabitants in New Zealand at 31 March 2006, compared to 30.2 subscribers per 100 at 30 September 2005. The number of non-analog subscribers in New Zealand increased from 9.0 per 100 inhabitants at the end of September 2005 to 11.5 per 100 inhabitants at the end of March 2006. The OECD average at December 2005 was 13.6 per 100 inhabitants.

New Zealand non-analog subscribers increased by 2.5 subscribers per 100 inhabitants, compared to an OECD average increase of 1.8. Although the number of non-analog Internet subscribers per 100 inhabitants has increased in the six months to 31 March 2006, New Zealand retains the same OECD subscriber ranking that it had at 30 September 2005 (22nd).

Internet Service Provision in New Zealand

For the six months ended 31 March 2006, there were 57 ISPs operating in New Zealand, down from 66 at 30 September 2005, a decrease of nearly 14%. Percentiles are a useful method for comparing ISP size over time. Percentiles are determined by sorting ISPs (by number of subscribers) from smallest to largest, then calculating subscriber numbers at intervals of 20%. In the year to 31 March 2006, ISPs at the 80th percentile increased their subscriber numbers, at the expense of ISPs at lower percentiles.



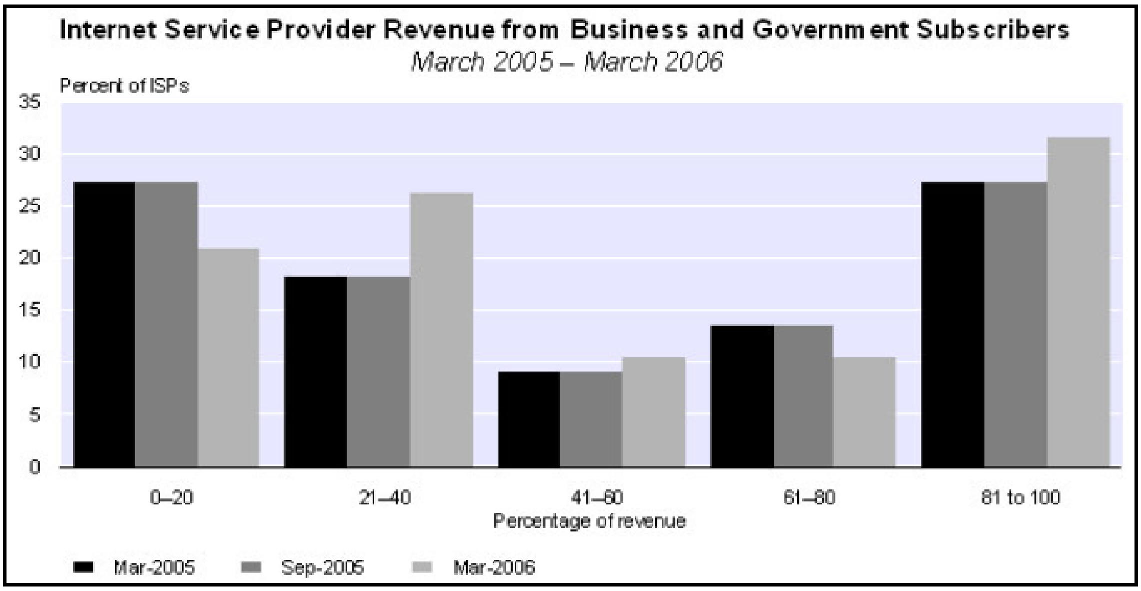
For the six months ended 31 March 2006, the total number of Internet subscribers increased 4% to approximately 1.29 million subscribers. While this is an increase of 49,000 subscribers from 30 September 2005, growth has slowed to 4%, down from the 7% increase recorded for the six months to 30 September 2005.

Business and government subscribers increased approximately 6% (13,800 subscribers) in the six months to 31 March 2006, down from the 17% increase for the six months to 30 September 2005. Residential subscribers increased by approximately 4%, compared with the 5% increase in the previous survey period.

For the six months ended 31 March 2006, residential subscribers accounted for about 82% of the total number of subscribers and provided 63% of ISP revenue. Business and government subscribers constituted 19% of the total number of active subscribers and 37% of ISP revenue.

ISP Revenue from Business and Government Subscribers

The proportion of revenue ISPs received from business and government subscribers (as opposed to the proportion of revenue received from residential subscribers) at 31 March 2006 was similar to that at 30 September 2005. In the six months ended 31 March 2006, 21% of ISPs received between 0% and 20% of their revenue from business and government subscribers and a further 32% of ISPs received between 81% and 100% of their revenue from business and government subscribers. There was an 8% increase in the number of ISPs that received between 21% and 40% of their revenue from business and government subscribers.



Internet Subscriber Download Speeds

At 31 March 2006, the predominant download speed category was less than 64kbps, with 806,600 active subscribers, which is a decrease of nearly 5% from 30 September 2005.

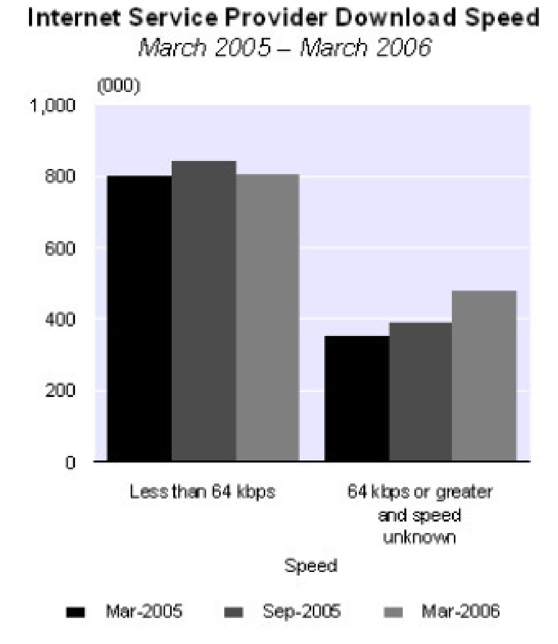
There were 481,300 subscribers whose design download speed was 64kbps or greater at 31 March 2006, a 23% rise from the 392,600 subscribers recorded at 30 September 2005. Within this category, download speeds of between 128kbps and 256kbps were the most common, having increased between 0% and 10% from 30 September 2005. The next most common download speed categories in descending order were: 2mbps to 10mbps, 512kbps to 2mbps, 256kbps to 512kbps, 10mbps or greater, 64kbps to 128kbps and unknown download speed.

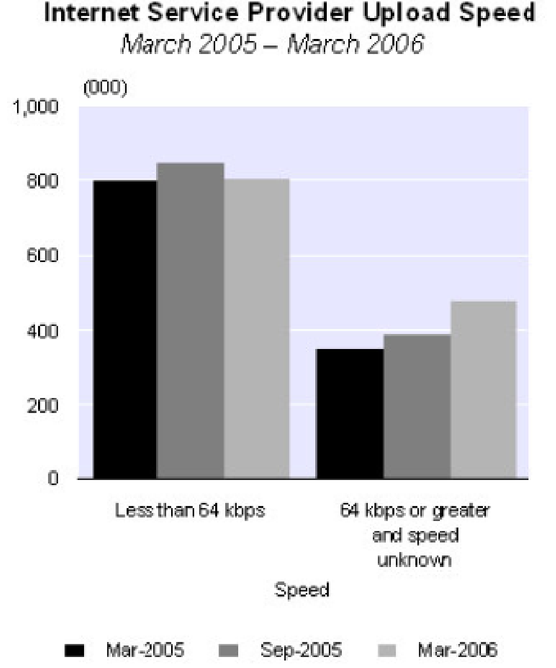
Internet Subscriber Upload Speeds

There were 806,600 subscribers in the predominant upload speed category of less than 64kbps at 31 March 2006, down nearly 5% from 30 September 2005.

Subscribers whose design upload speed was 64kbps or greater increased 23% from the 30 September 2005 to 481,300 subscribers at 31 March 2006. Within this category, upload speeds of between 128kbps to 256kbps remained the most common. The next most common upload speeds in descending order were: 256kbps to 512kbps, 512kbps to 2mbps, 64kbps to 128kbps, 2mbps to 10mbps, 10mbps or greater and unknown upload speed.

Although there has been a large amount of volatility in upload speed categories, the rankings are unchanged.



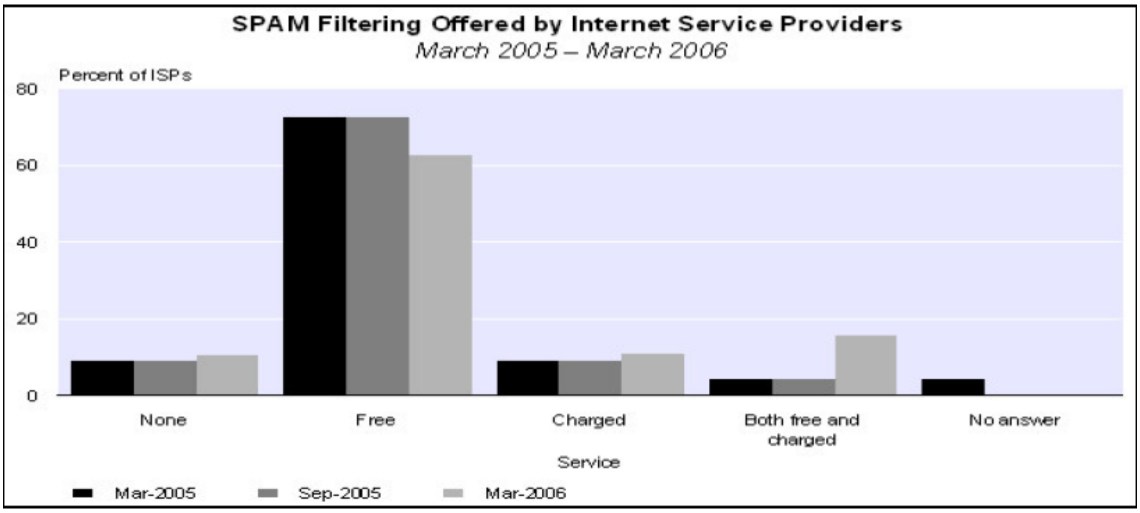


Filtering Services Supplied by Internet Service Providers

It should be noted that the Internet Service Provider Survey March 2006 only measures the uptake of filtering services by subscribers where the service is supplied by the ISP. There are many other alternatives available to subscribers, including purchasing or downloading software.

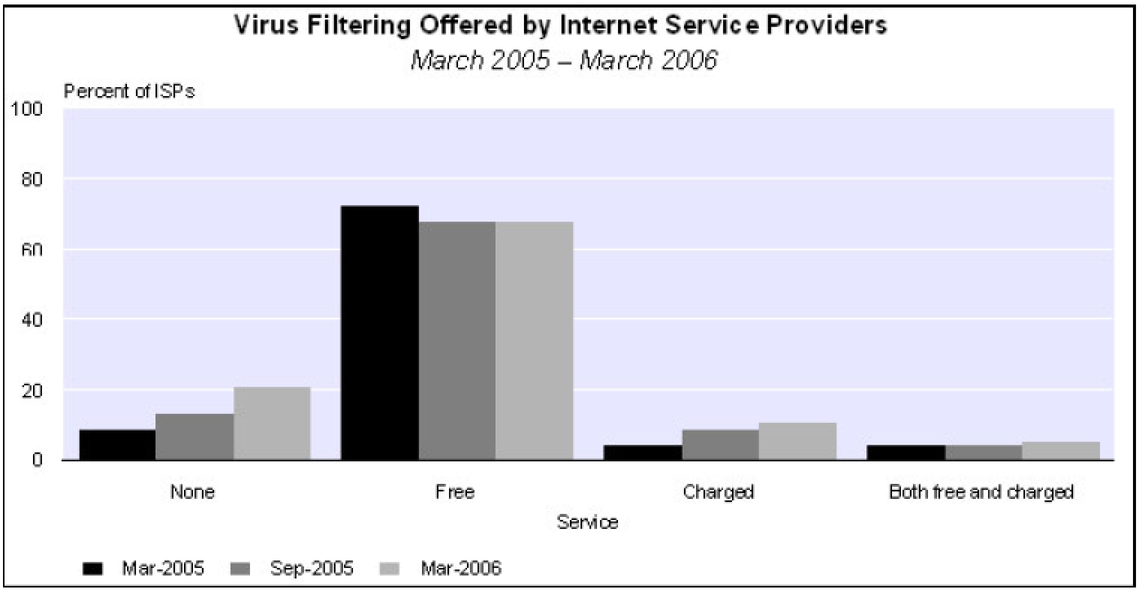
Spam Filtering

At 31 March 2006, 1,157,800 (90% of) Internet subscribers had adopted a spam-filtering product offered by their ISP. Ninety percent of ISPs offered their subscribers a spam-filtering service. Of those ISPs, 63% provided spam filtering as a free service and 11% provided spam filtering as a charged service. A further 16% of ISPs provided spam filtering as both a free and changed service, depending on the Internet access plan.



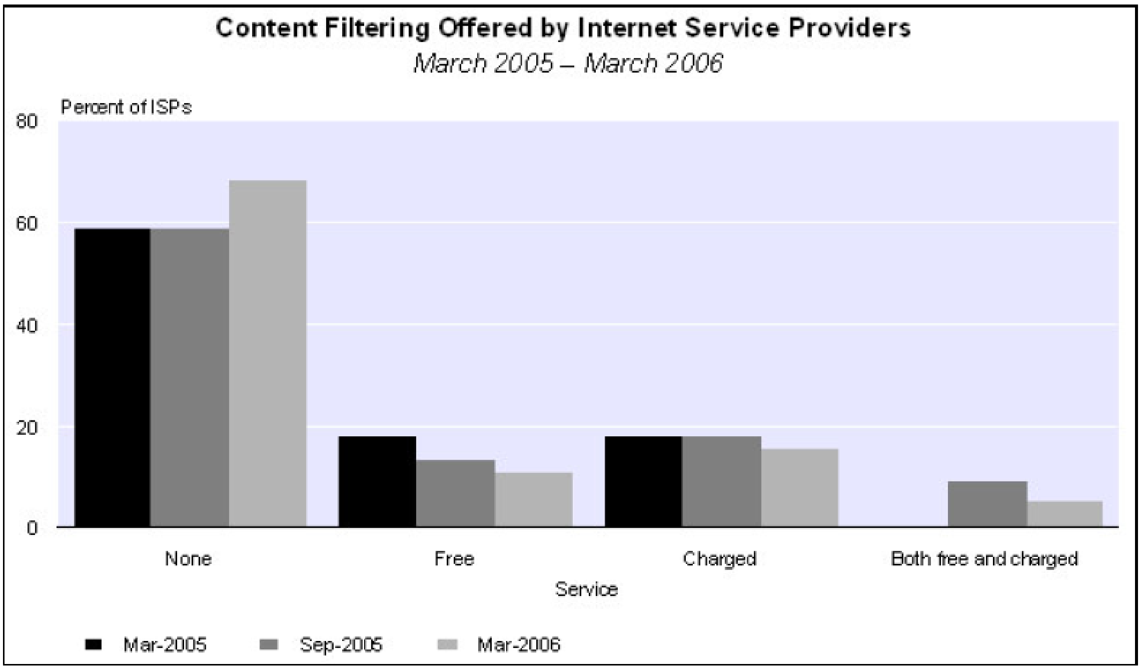
Virus Filtering

A total of 1,166,100 (91% of) Internet subscribers had adopted a virus-filtering service offered by their ISP at 31 March 2006. A total of 84% of ISPs offered their subscribers a virus-filtering service. Of those ISPs, 68% provided virus filtering as a free service and 11% offered virus filtering as a charged service. A further 5% of ISPs provided virus filtering as both a free and charged service, depending on the Internet access plan.



Content Filtering

At 31 March 2006, 68% of ISPs offered no content-filtering services and 32% of ISPs offered their subscribers a content-filtering service. Of those ISPs, 11% provided content filtering as a free service and 16% provided content filtering as a charged service. A further 5% of ISPs provided content filtering as both a free and charged service, depending on the Internet access plan.

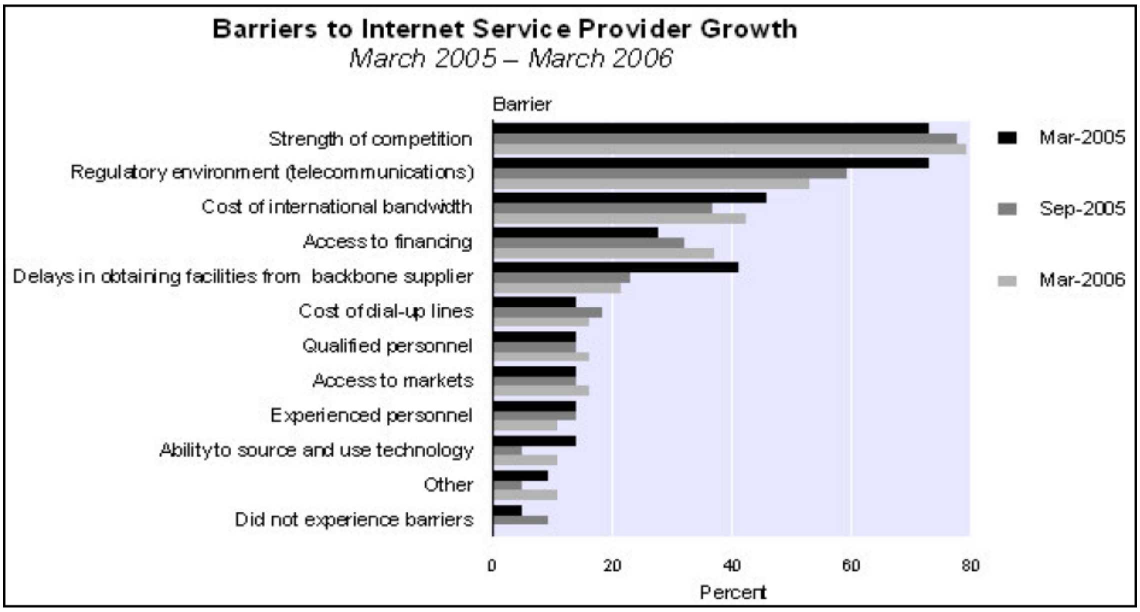


Internet Service Provider Barriers to Growth

For the six months ended 31 March 2006, 79% of ISPs in New Zealand saw the strength of competition as the greatest barrier to the growth of their operations. Other common barriers to growth identified were the regulatory environment relating to telecommunications (53%), the cost of international bandwidth (42%), and ISPs' access to financing (37%).

At 31 March 2006 all ISPs identified barriers to growth, whereas at 30 September 2005 9% of ISPs said there were no barriers to growth. Over the same period there was a 6% decrease in the number of ISPs reporting that the regulatory environment relating to telecommunications was a barrier to growth and there was a 6% increase in the number of ISPs reporting other barriers.

In the year to March 2006, there was a 20% decrease in the number of ISPs reporting that the regulatory environment relating to telecommunications was a barrier to growth, and 20% fewer ISPs reported that delays in obtaining facilities from the backbone supplier was a barrier to growth.



CCIP Relationship with New Zealand ISPs
The CCIP currently has a basic working relationship with two major New Zealand ISPs.

6-2. National Policy and law on Information Security

The security policy and guidance website (www.security.govt.nz) provides information on the national information security policy.

The website (www.gcsb.govt.nz/infosec) acts as a focal point for the publication of government information about security standards, procedures, and resources.

Legal Framework

- Telecommunications (Intercept Capability) Act 2004
- Crimes Amendment Act 2004
- Electronic Transaction Act
- Government Communications Security Bureau Act 2003
- Review of Telecommunications Act 2001
- Terrorism Suppression Act 2002
- Civil Defence and Emergency Management Act 2002

Telecommunications (Intercept Capability) Act 2004
Telecommunication Network Operators are required to maintain an interception capability to:

- Identify and intercept telecommunications, authorised under an interception warrant;
- Obtain call associated data;
- Protect the privacy of other telecommunication users.

Crimes Amendment Act 2004
The Crimes Amendment Act 2003 came into force on 1 October 2003 and creates four new offences:

- Accessing a computer system for a dishonest purpose;
- Damaging or interfering with a computer system;

- Making, selling, or distributing or possessing software for committing crime;
- Accessing a computer system without authorisation.

Electronic Transaction Act

The ETA facilitates the use of electronic technology by:

- Confirming electronic methods of communication are legally effective;
- Sets default rules for the time and place of dispatch and receipt of electronic communications (whether or not the communications are used to meet statutory requirements);
- Provides that certain paper-based legal requirements may be met by using electronic technology that is functionally equivalent to those legal requirements.

Government Communications Security Bureau (GCSB) Act 2003

The Act defines the GCSB's principal functions in a technology-neutral manner. In addition to the comprehensive description of the GCSB's functions, the Act:

- formally establishes the GCSB as a statutory agency of government;
- defines the appointment, functions and powers of the Director of the GCSB;
- provides for the issue of interception warrants; and
- ensures consistency with other NZ legislation.

Review of Telecommunications Act 2006

- Schedule 3 Investigations into:
  - unbundling the local loop network; and
  - mobile termination.

Terrorism Suppression Act 2002

The law:

- criminalises terrorist bombings and the financing of terrorist organisations;
- makes it an offence to recruit and take part in a terrorist movement;
- allows funding to be frozen and forfeited;
- enhances the powers of border agencies to participate in international information exchange;
- strengthens extradition measures;
- criminalises terrorist attacks on the food chain and New Zealand's biosecurity; and
- the law also covers the unlawful possession of plastic, explosive and nuclear material.

Civil Defence and Emergency Management Act 2002

The Civil Defence Emergency Management Act 2002 replaces the Civil Defence Act 1983. The new Act:

- promotes sustainable management of hazards;
- encourages and enables communities to achieve acceptable levels of risk;
- provides for planning and preparation for emergencies, and for response and recovery;
- requires local authorities to coordinate planning and activities;
- provides a basis for the integration of national and local civil defence emergency management; and
- encourages coordination across a wide range of agencies, recognizing that emergencies are multi-agency events.

Unsolicited Messaging Bill 2006

The Unsolicited Messaging Bill 2006 will legislate against unsolicited electronic messages sent for marketing or promotional purposes (SPAM).

- Penalties: $200,000 (NZD) for individuals / $500,000 (NZD) companies

6-3. CERT Services and Statistics on Malicious Activities

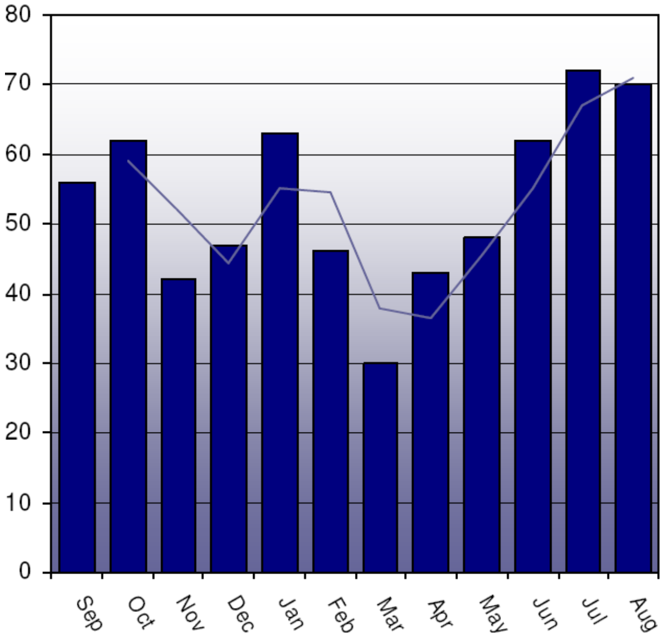
Currently, there is no New Zealand National CERT.

AusCERT is the defacto New Zealand CERT for many New Zealand organisations and departments.

The CCIP works closely with AusCERT regarding malicious activities and with NISSC/UNIRAS (UK) on matters related to Critical Infrastructure Protection.

CCIP Statistics on Malicious Activity

CCIP Operations Centre Activity



August saw a high number of advisories posted on the CCIP website, including a number that were deemed critical. The number of alerts being sent directly via the CCIP mailing lists remained steady at 2 during the month. Advisories posted during the month of major significance included:

Apple Security Update 2006-004, NZ computer Crime & Security Survey published by Otago University, MS06-042: Cumulative security update for Internet Explorer, Microsoft Internet Explorer URL Parsing Buffer Overflow Vulnerability, and of course the Microsoft Security Bulletin Summary for August 2006 which was released on the 9th August.

The graph to below represents the number of advisories posted by the CCIP Operations Centre over the last 12 months.

CCIP e-Bulletins

CCIP issued 3 e-Bulletins in the month of August. Below are links to these publications and a sample of the articles included in each.

Issue 22 ~ 4th August 2006

- The Pharming Guide - Understanding & Preventing Pharming Attacks

- The State of Spam
- After an Exploit: Mitigation & Remediation
- SPI Dynamics Warns of Potential Cross-Site Scripting Attack

Issue 23 ~ 15th August 2006

- New Zealand Computer Crime & Security Survey
- 2006 NetSafe Symposium - CyberSafety & Security Online
- Policy Review – Registering, Managing & Canceling Domain Names
- Surviving the Monthly Patch Cycle

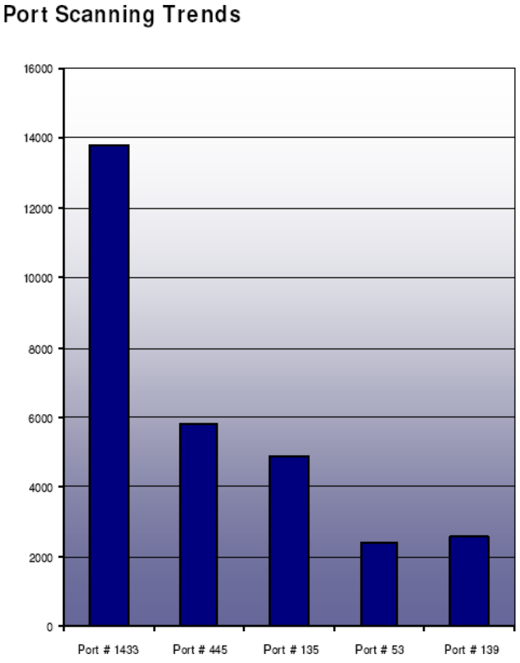
Issue 24 ~ 23rd August 2006

- Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors
- Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP
- The 10 Biggest Myths of IT Security
- Battling Image Spam

e-Bulletins are sent to members of the CCIP mailing lists. Back issues can be obtained by visiting the 'Publications' page on the CCIP website.

Port Scanning

Wikipedia definition: A port scanner is a piece of software designed to search a network host for open ports. This is often used by administrators to check the security of their networks and by crackers to compromise it. The Port Scanning Trends Graph to the right outlines the number of recorded attacks against each of the 5 highest attacked ports for the month. For more information regarding Port Scanning, please visit the Internet Storm Centre.

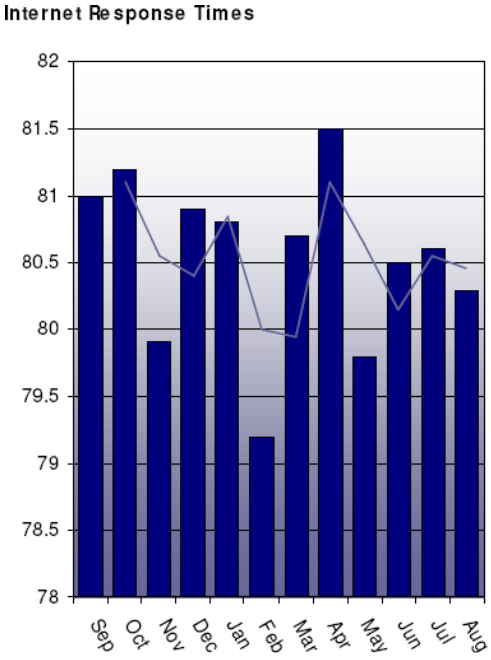


Internet Response Times

Internet Response trends for the month of August remained relatively steady, with the New Zealand router response time remaining at a steady average of 190ms, giving an overall Traffic Index average of 80.

The graph to the right represents the response time of a New Zealand monitored router (b2.sxb.tsnz.net - 203.98.39.129) as a traffic index. The higher the index, the lower the response time, and therefore representing better performance and reliability of the connection.

For more information regarding Internet Response Times, please refer to the Internet Traffic Report websites

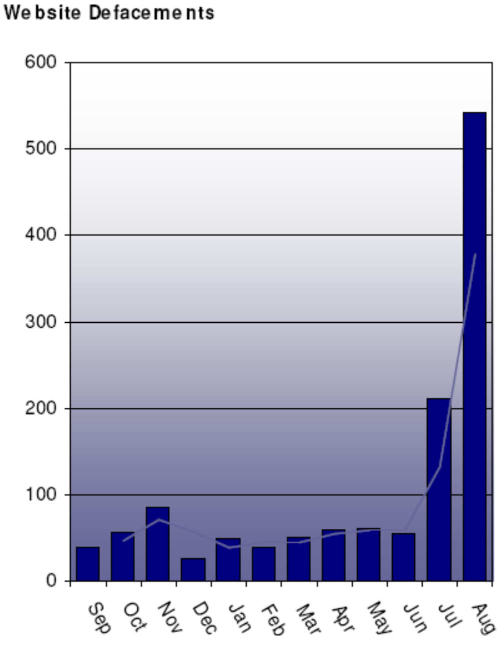


Website Defacements

Defacements of New Zealand Websites for the month of August continued the recent upward trend, with a record setting 544 reported defacements. This is an average of 10 times the normal monthly total for reported defacements, and dragged the average number of defacements for the last 12 months up to 106 per month - well above the normal monthly average of 52 defacements. This primarily was a result of a single mass defacement reported on 7th August consisting of 354 different URL's.

The graph to the right indicates the number of reported website defacements against New Zealand sites recorded by the CCIP Operations Centre during the past 12 months.

For more information regarding website defacements, please refer to the zone-h websites.



7. Viet Nam

7-1. Internet Usage Statistics

As of July 2007:

- Number of convert subscribers: 4,671,049
- Internet Users: 16,737,129
- Penetration ratio: 20.14%
- Total Internet bandwidth: 10,508 Mbps
- Total number of .vn domains: 46,445
- Total number of IP Address: 3,786,496
- Number of broadband subscribers: 876,056

There are total 9 ISPs in Viet Nam.

VNPT	2,397,221	51.32%
FPT	851,386	18.22%
VIETTEL	783,463	16.77%
EVN	257,644	5.51%
SPT	191,737	4.10%
OCI	108,530	2.32%
NETNAM	79,302	1.69%
TIENET	1,279	0.02%
HPT	487	0.01%

(Source: http://www.thongkeinternet.vn)

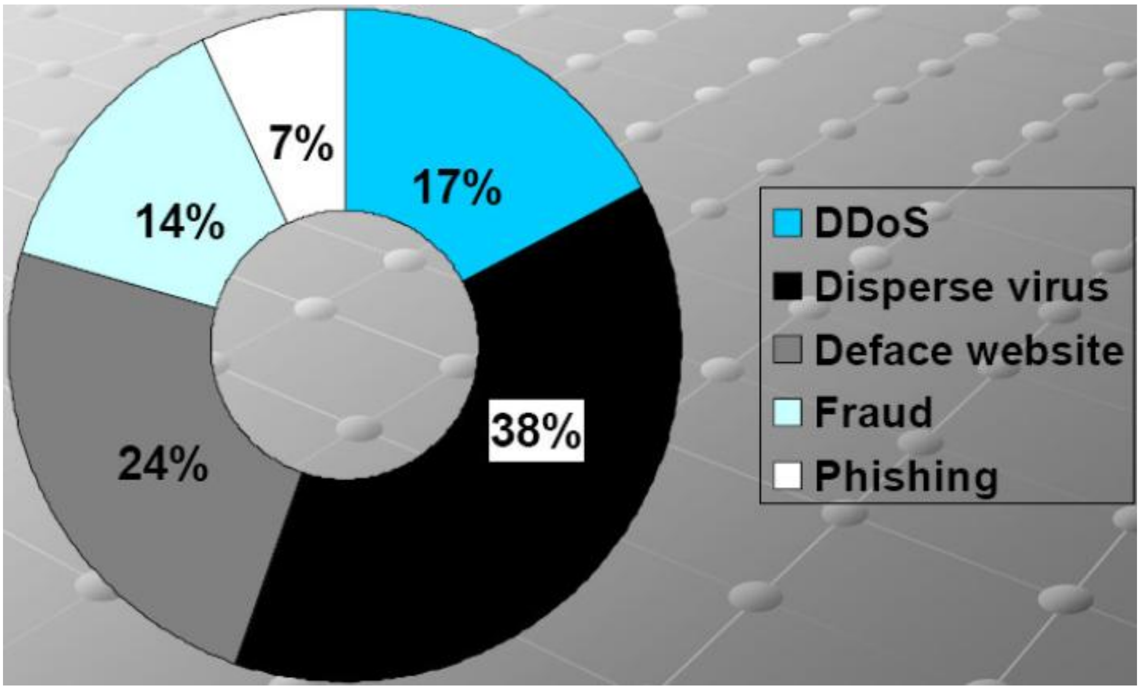
7-2. National Policy and Law on Information Security

- Electronic Transaction Law had been passed by the National Assembly on 29/11/2005. This Law regulates electronic transactions within government agencies, civil and business activities.
- Law on Information Technology was promulgated at 9th Session of the National Assembly's Legislature XI on 29 June 2006. This law becomes effective as of 1st January 2007.
- Decree No. 64 promulgated on 10/4/2007 regulated the application IT in operations of government agencies
  - There are many provisions about information security. Emphasize the role of infosec.

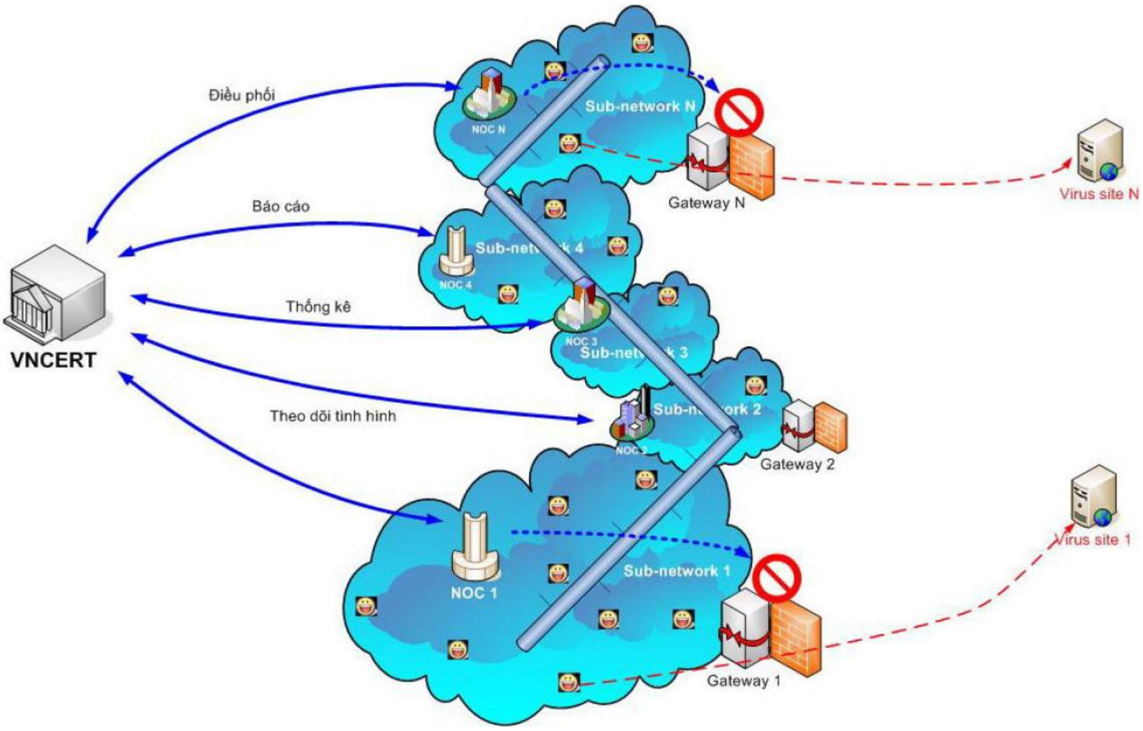
7-3. CERT Services and Statistics on Malicious Activities

- Deploy IHS (Incident Handling System)
- Cooperation on remove phishing sites
- Provide security applications, solutions, standards
- Release security publications
- Provide assessment service for network security of information systems and products
- Inspection, assessment, and admit service to organizations achieving security standard
- Organize services about security training, testing and providing certificate about security

Statistics on malicious activities



7-4. Information on Constituency


Điều phối
Báo cáo
Thống kê
Theo dõi tình hình
VNCERT
NOC N
Sub-network N
Gateway N
Virus site N
Sub-network 4
NOC 4
NOC 3
Sub-network 3
Sub-network 2
NOC 2
Gateway 2
NOC 1
Sub-network 1
Gateway 1
Virus site 1