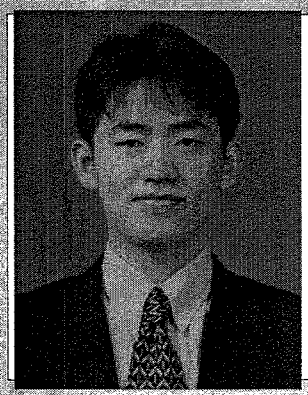
Policies in Addressing Cyber Threat

검찰
PROSECUTORS' OFFICE

18. Nov. 2009.

2nd APEC seminar on Protection of Cyberspace from Terrorist Use and Attacks

SPEAKER : CHULSOO KIM



- 1995. 2. Graduated SEOUL National University
- 2001. 5.~Present, Working as a Prosecutor
- 2009. 11. Participated in ASEAN Workshop on Enhancing Cybercrime capacity held in Indonesia

- National Security Part in Seoul Northern District Prosecutors' Office
- Mainly dealing with Planning related to Office Management

CONTENTS

1. Introduction

朝鮮日報

2009년 07월 08일 수요일 A03면 종합

국가기관·은행·신문 … 누군가 '의도적인 공격'

朝鮮日報

2009년 07월 08일 수요일 A01면 종합

주요 사이트에 동시다발 '사이버테러'

청와대·국회·국방부·한나라당·조선닷컴·네이버 등… 어제 저녁 수시간씩 장애

청와대와 조선닷컴, 네이버, 신한·외환은행 등 국내의 주요 대형 인터넷 사이트들이 동시에 해킹을 당해 7일 저녁 4시간여 동안 접속되지 않는 '인터넷 대란'이 발생했다. 국적 불명의 미확인 해커가 저지른 사이버 테러로 인해 1000만명 이상의 인터넷 가입자들이 해당 사이트에 접속하지 못해 큰 불편을 겪었다. 여러 사이트 서버를 통합관리하는 인터넷데이터센터(IDC)가 사이버 테러를 당해 해당 서비스가 중단된 적은 있었으나, 각 분야의 대표 사이트들이 동시다발적으로 공격당한 것은 이번이 처음이다. 관련기사 A3면

7일 오후 6시가 넘어서면서 조선닷컴을 비롯해 청와대와 국회, 국방부, 한나라당, 포털사이트 네이버의 이메일·블로그, 옥션, 신한은행과 외환은행 등 국내 주요 사이트들은 서버스 접속이 아예 안되거나 극도로 느려지는 상태에 빠져 대혼란을 겪었다. 한국의 주요 기관 사이트에 해킹이 발생하면서 한·미 당국간 협의에 따라 한국에서 미 백악관·국무부 등 정부 사이트 접속이 일시적으로 차단됐다. 국내 사이트들은 오후 10시30분부터 정상화 상태에 들어갔지만 일부는 새벽까지 접속장애가 계속됐다.

조선닷컴은 오후 6시30분쯤부터 정체불명의 접속자가 급증하면서 적정용량을 초과해 접속 불능상태에 빠졌다. 네이버도 "오후 6시50분쯤부터 일부 게임 블로그와 메일 서비스의 접속이 원활하지 않은 오류가 간헐적으로 발생했다"고 밝혔다.

국가정보원 등 국내 유관기관들과 인터넷 업계에서는 특정 해커집단이 각 분야의 대표 사이트들을 정해 DDoS(분산서비스거부공격·키워드 참조)를 한 것으로 추정하고 있다. 국가정보원은 이번 사태의 원인 파악과 대책마련에 나서는 동시에 해킹세력에 대한 추적에 나섰다고 관계자가 밝혔다.

청와대 관계자는 "중국 쪽에서 해킹 공격이 있는 것으로 추정돼 조사 중"이라고 말했다. 한 정부 관계자는 "보안이 엄격한 주요 사이트를 선별해 공격한 것으로 봐서 넷트워크 장악기술이 뛰어난 해커그룹이 의도적으로 사이버테러를 저지른 것으로 추정된다"고 말했다. 김회성 기자 freman@chosun.com

강경수 기자 nomad586@chosun.com

성이 높다"고 말했다.

뿐만 아니라 정부 당국은 국내 사이트에 대한 공격에 앞서 미국 백악관·국무부·국방부 등 해외 주요 기관에 대한 공격도 최근 수차례 시도된 것으로 이야기하기 힘들지만, 누군가가 특정 사이트만 공격해 공격한 것은 분명해 보인다"고 말했다.

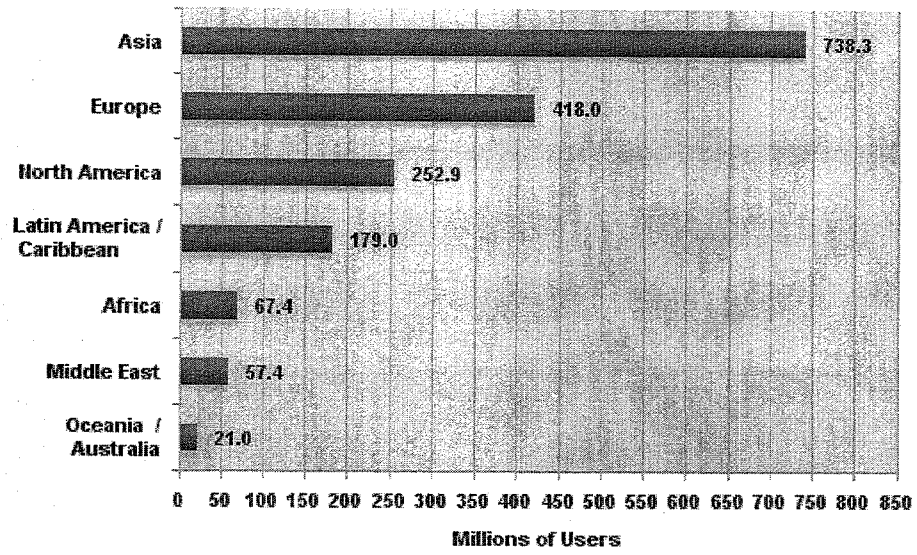
조형래 기자 hrcho@chosun.com

신경민 기자 sunny@chosun.com

신한은행 홈페이지는 오후 6시30분쯤부터 접속이 폭주해 접속이 안 되고 인터넷 뱅킹 속도가 느려지는 등 인터넷 장애가 발생했다. 신한은행 측은 "비정상적 접속이 많아난 IP를

2. Status for Cyber Threat

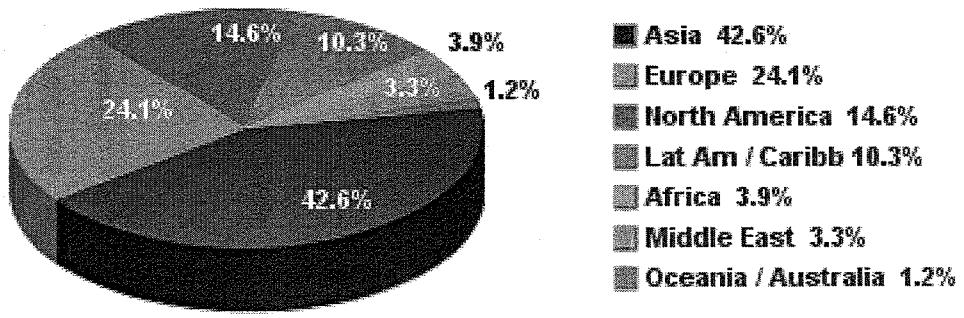
Internet Users in the World by Geographic Regions



Source: Internet World Stats - www.internetworldstats.com/stats.htm
Estimated Internet users are 1,733,993,741 for September 30, 2009

2. Status for Cyber Threat

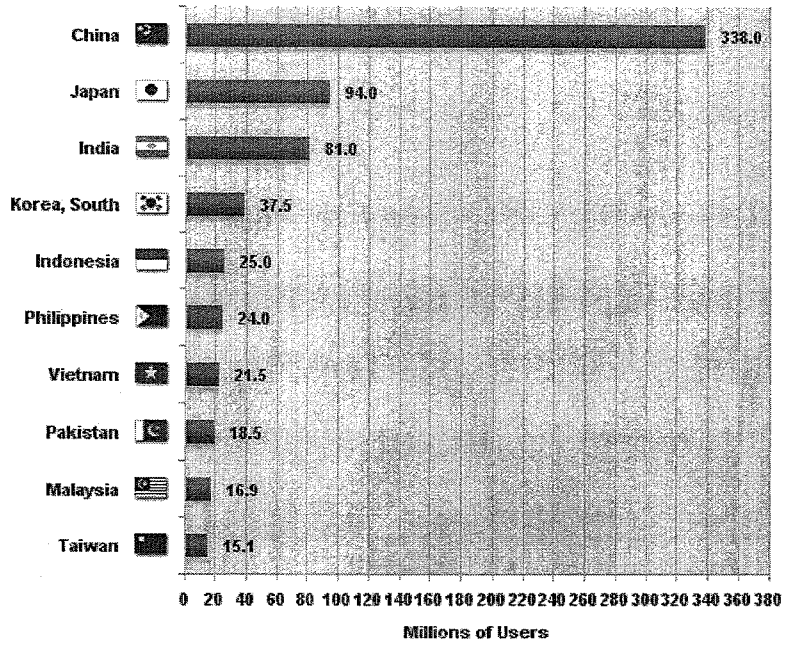
World Internet Users by World Regions



Source: Internet World Stats - www.internetworldstats.com/stats.htm
1,733,993,741 Internet users for September 30, 2009

2. Status for Cyber Threat

Asia Top 10 Internet Countries - 2009 Q2

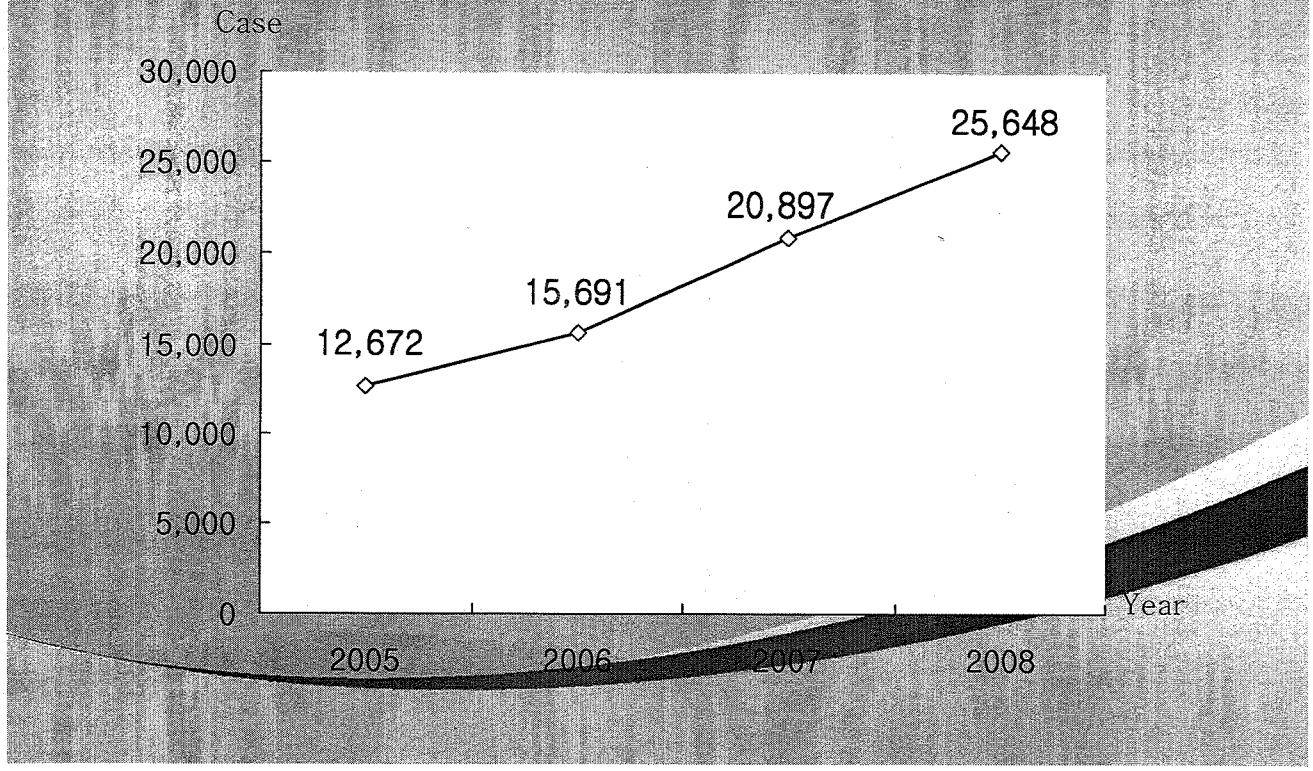


Source: Internet World Stats - www.internetworldstats.com/stats3.htm
Estimated Asia Internet users 704,213,930 for 2009 Q2

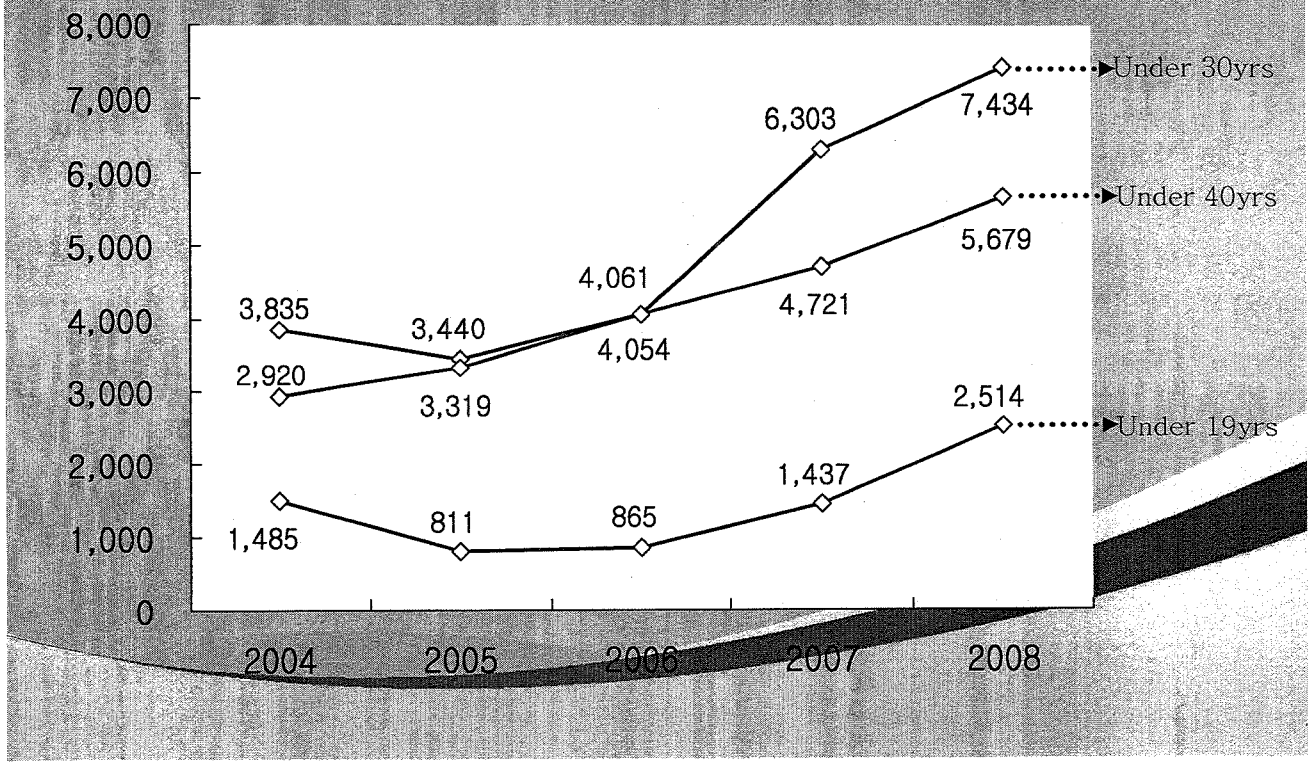
2. Status for Cyber Threat

ASIA	Population (2009 Est.)	Internet Users, (Year 2000)	Internet Users, Latest Data	Penetration (% Population)	User Growth (2000-2009)	Users (%) in Asia
Afganistan	28,395,716	1,000	500,000	1.8 %	49,900.0 %	0.1 %
Armenia	2,967,004	30,000	172,800	5.8 %	476.0 %	0.0 %
Azerbaijan	8,238,672	12,000	1,500,000	18.2 %	12,400.0 %	0.2 %
Bangladesh	156,050,883	100,000	500,000	0.3 %	400.0 %	0.1 %
Bhutan	691,141	500	40,000	5.8 %	7,900.0 %	0.0 %
Brunei Darussalem	388,190	30,000	187,900	48.4 %	526.3 %	0.0 %
Cambodia	14,494,293	6,000	70,000	0.5 %	1,066.7 %	0.0 %
China *	1,338,612,968	22,500,000	338,000,000	25.3 %	1,402.2 %	48.2 %
Georgia	4,615,807	20,000	360,000	7.8 %	1,700.0 %	0.1 %
Hong Kong *	7,055,071	2,283,000	4,878,713	69.2 %	113.7 %	0.7 %
India	1,156,897,766	5,000,000	81,000,000	7.0 %	1,520.0 %	11.6 %
Indonesia	240,271,522	2,000,000	25,000,000	10.4 %	1,150.0 %	3.6 %
Japan	127,078,679	47,080,000	94,000,000	74.0 %	99.7 %	13.4 %
Kazakhstan	15,399,437	70,000	1,900,600	12.3 %	2,615.1 %	0.3 %
Korea, North	22,665,345	-	-	-	-	0.0 %
Korea, South	48,508,972	19,040,000	37,475,800	77.3 %	96.8 %	5.3 %
Kyrgystan	5,431,747	51,600	750,000	13.8 %	1,353.5 %	0.1 %
Laos	6,834,345	6,000	100,000	1.5 %	1,566.7 %	0.0 %
Macao *	559,846	60,000	238,000	42.5 %	296.7 %	0.0 %
Malaysia	25,715,819	3,700,000	16,902,600	65.7 %	356.8 %	2.4 %
Maldives	396,334	6,000	71,700	18.1 %	1,095.0 %	0.0 %
Mongolia	3,041,142	30,000	320,000	10.5 %	966.7 %	0.0 %
Myanmar	48,137,741	1,000	40,000	0.1 %	3,900.0 %	0.0 %
Nepal	28,563,377	50,000	397,500	1.4 %	695.0 %	0.1 %
Pakistan	174,578,558	133,900	18,500,000	10.6 %	13,716.3 %	2.6 %
Philippines	97,976,603	2,000,000	24,000,000	24.5 %	932.5 %	2.9 %
Singapore	4,657,542	1,200,000	3,104,900	66.7 %	158.7 %	0.4 %
Sri Lanka	21,324,791	121,500	1,148,300	5.4 %	845.1 %	0.2 %
Taiwan	22,974,347	6,260,000	15,143,000	65.9 %	141.9 %	2.2 %
Tajikistan	7,349,145	2,000	484,200	6.6 %	24,110.0 %	0.1 %
Thailand	65,998,436	2,300,000	13,416,000	20.3 %	483.3 %	1.9 %
Timor-Leste	1,131,612	-	1,500	0.1 %	0.0 %	0.0 %
Turkmenistan	4,884,887	2,000	70,000	1.4 %	3,400.0 %	0.0 %
Uzbekistan	27,606,007	7,500	2,416,000	8.8 %	32,113.3 %	0.3 %
Vietnam	88,576,758	200,000	21,524,417	24.3 %	10,662.2 %	3.1 %

2. Status for Cyber Threat



2. Status for Cyber Threat



3. Cyber Threat Addressing System

Investigation { Prosecutors'Office / Police

Public Sector	Private Sector
· NCSC(National Cyber Security Center) in NIS(National Intelligence Service) · KCC(Korea Communications Commission) · KISA(Korea Internet & Security Agency) · CRMO(Central Radio Management Office) · Local Government	Kr-CERT(Computer Emergency Response Team) in KISA

3. Cyber Threat Addressing System

< Public Security Area >

SPO	Seoul Central DPO	Other DPOs
1st, 2nd, 3rdDivision	1st, 2nd Department	8 Departments

3. Cyber Threat Addressing System

< Cyber Crime Area >

	SPO	Seoul Central PPO	other DPOs
1996	ICTF (Task Force)		
2000	CCID (Division)	CCID (Department)	(1997~2003) 23 CCISs (Squad)
2001	ICIC	ICIC	
2005	DFD (Digital Forensic)	HCID (High-Tech Crime)	
2008	DFC		
2009		1st , 2nd HCID	

3. Cyber Threat Addressing System

A. Criminal Law

- Interruption of Business, Deletion of Data, Forgery of Public Records, etc

B. Act on Promotion of Information and Communication Network Utilization and Information Protection

- Threats involving cyber-crime such as DDoS

C. Act on Information and Communication Infrastructure Protection

- Crimes bringing about damages to infrastructure

4. Policies to Enhance Cyber Security

A. Digital Forensic Cyber Sheriff Course

- Period : 10months
- Object : Prosecution Investigation Officer
- Curriculum

  a. Basic education : internet management, etc

  b. Practical education : operation of digital evidence analysis program, etc

4. Policies to Enhance Cyber Security

B. Encouraging the Experts on Section

- Field : Accounting Analysis, Asset Recovery, Advanced Interrogation technique, etc
- DB to the Experts on Section

4. Policies to Enhance Cyber Security

C. Special Employment of Outside Expert

- Field : Cryptogram Analysis, Network Analysis, DB Analysis etc
- Joint Research Project between the Public & Private Sector

4. Policies to Enhance Cyber Security

D. Acquisition of Advanced Investigation Technique

- Participation at Training Program, Academic Symposium, Conference in Advanced Countries
- Benchmarking the Anti-Cyber Threat System of the Advanced Countries

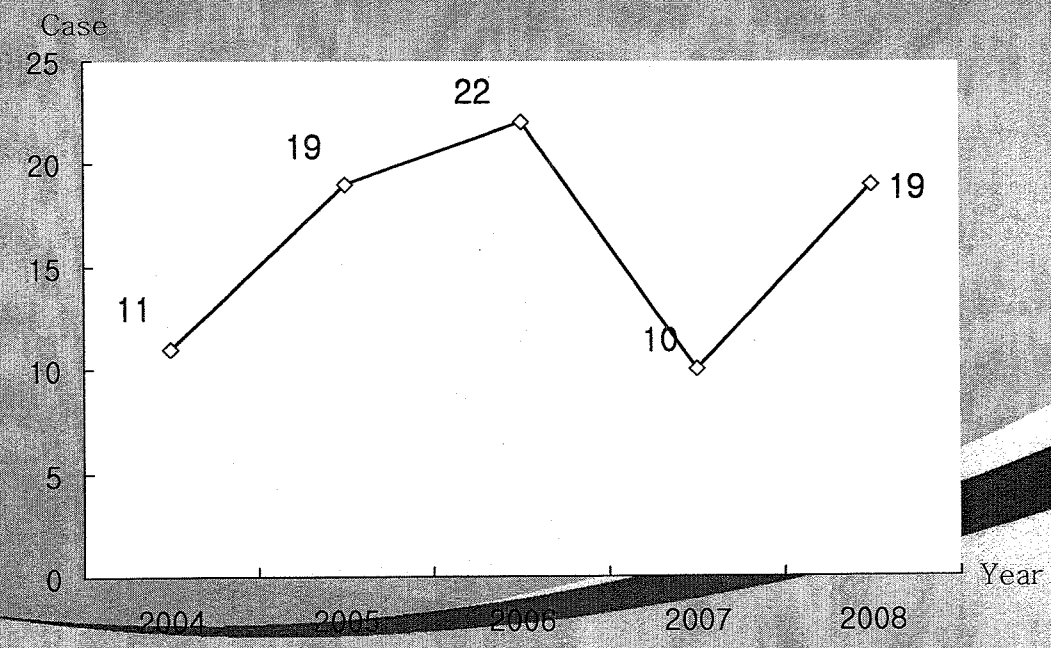
4. Policies to Enhance Cyber Security

E. Activation of International Cooperation

- The G8's Network of 24Hour Contacts for International High-Tech Crime
  - Cooperation with U.S. and U.K. at the DDoS attack occurred on July. 7. 2009
- the Council of Europe 's Cyber Crime Convention

4. Policies to Enhance Cyber Security

< Statistics of International Copperation >



5. Conclusion

- The Characteristic of Cyber Threat
  - Trans-national Threat
  - Unprecedented types of Threat
- Need for International Cooperation
  - Common Archival Processing of the Electronic Evidence
  - Timely Mutual Assistance System