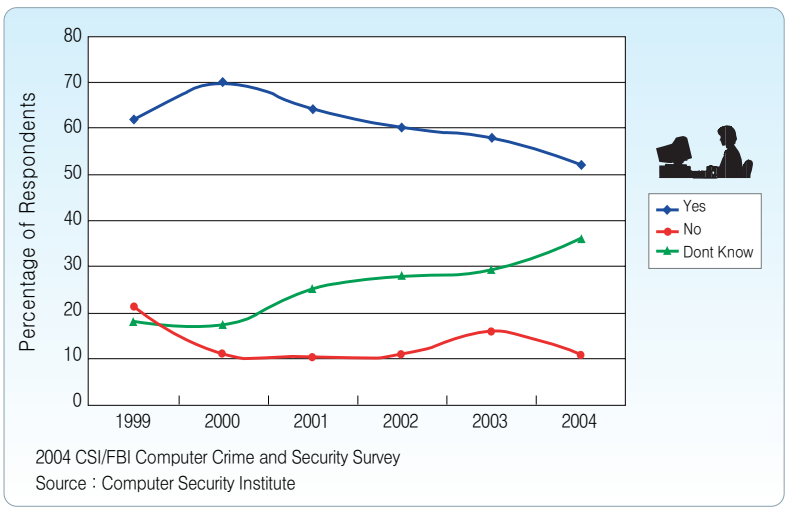
왜 한국에는 유명한 해커그룹이 없을까?

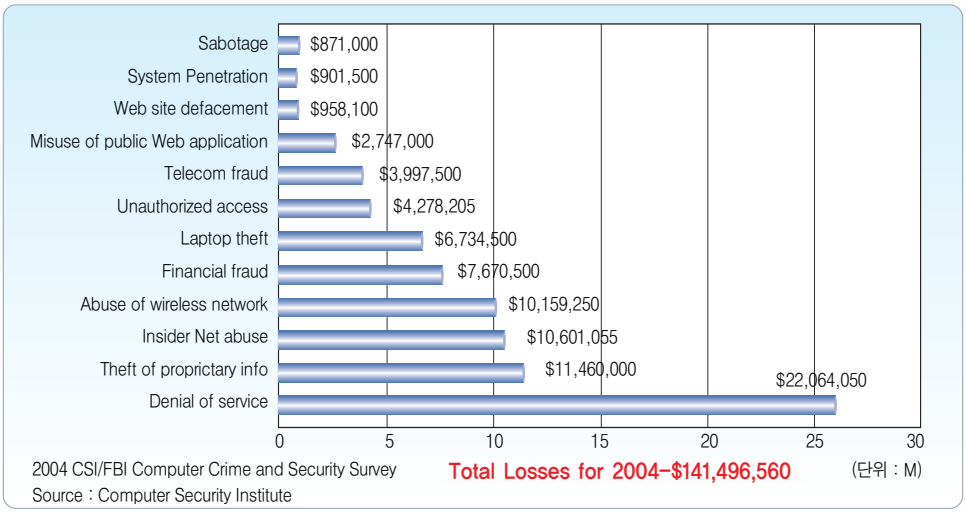
충남대 해킹 · 보안 동아리 Argos 1기 회장 **최 효 식**
(drwx@argos.or.kr)

1. Hacker! 그들은 어디(where)에서 무엇(what)을 하고 있는가?

인터넷 침해사고의 건수와 그에 따른 금전적인 피해는 국내외적으로 계속해서 증가하고 있다. 그럼에도 불구하고, 일반인들은 인터넷 침해로 인한 위험성에 대해 제대로 인지하고 있지 못할 뿐만 아니라 자신과는 상관없는 일처럼 생각하고 있다. [그림 1] 하지만, 미국의 예를 보면 2004년 한 해 동안의 인터넷 침해에 의한 금전적 손실은 막대했으며 [그림 2], 주요 기간 통신망의 장애로 인한 서비스 불능 사태가 여러 차례 발생하는 등 현재의 보안 환경은 심각한 위기 상황이라고 할 수 있다. 일반인들은 이런 침해 행위를 해커들의 소행이라고 판단하고, 해커들의 근거지를 추적하여 해커들의 악의적인 행위를 막아야 한다고 주장한다. 하지만, 누가 해커인가에 대한 명백한 정의와 이해가 선행되지 않고서는 컴퓨터 전문가들이 말하는 선의의 해커(Whitehat)에게 피해를 줄 수 있는 상황이 발생할 수도 있다. 따라서 크래커(Cracker)와 해커(Hacker)에 대한 구분을 명백히 할 필요가 있으며, 국내외 해커그룹의 동향을 파악함으로써 현재와 미래의 해커들의 기술적, 이념적 변화의 모습을 파악하고 예상할 수 있을 것이다. 과연 해커! 그들은 어디에서 무엇을 하고 있는 것일까?



[그림 1] 인터넷 침해 위험성에 대한 인식 부족



[그림 2] 인터넷 침해에 의한 손실액

2. 해커들의 움직임과 해커그룹

미국 정보보호 컨설팅 기관의 보고서에 의하면 [그림 3]과 같이 침해 시도 국가 TOP 20에 우리나라가 포함되어 있다. 침해 시도 국가의 선두권을 유지하고 있는 브라질, 미국, 중국의 공격 건수와는 많은 차이를 보이지만, 우리나라의 순위가 20위권 고려해 볼 때 국내에서 국외로의 공격 또한 적지 않게 발생하고 있음을 확인할 수 있다.

Top 20 - January 2003

Rank	Country	Code	Attacks
1	Brazil	BR	47
2	China	CN	22
3	Taiwan	TW	19
4	United States	US	17
5	Argentina	AR	6
6	Australia	AU	6
7	United Kingdom	GB	6
8	Turkey	TR	5
9	Egypt	EG	4
10	Costa Rica	CR	3
11	Jordan	JO	3
12	Korea, South	KR	3
13	Mexico	MX	3
14	Thailand	TH	3
15	Venezuela	VE	3
16	Ecuador	EC	2
17	Germany	DE	2
18	Indonesia	ID	2
19	Iran	IR	2
20	Peru	PE	2
	Others		16

Top 20 - Last 12 Months

Rank	Country	Code	Attacks
1	China	CN	203
2	United States	US	192
3	Brazil	BR	172
4	Turkey	TR	120
5	Taiwan	TW	92
6	Australia	AU	69
7	Mexico	MX	60
8	Nigeria	NG	59
9	Colombia	CO	42
10	United Kingdom	GB	36
11	Argentina	AR	35
12	Peru	PE	35
13	Bolivia	BO	29
14	El Salvador	SV	27
15	India	IN	26
16	Malaysia	MY	25
17	Morocco	MA	21
18	Poland	PL	21
19	Philippines	PH	20
20	Korea, South	KR	19
	Others		282

SIPS Report – January 2003
Source : mi2g.net

[그림 3] 침해 시도 국가 TOP 20

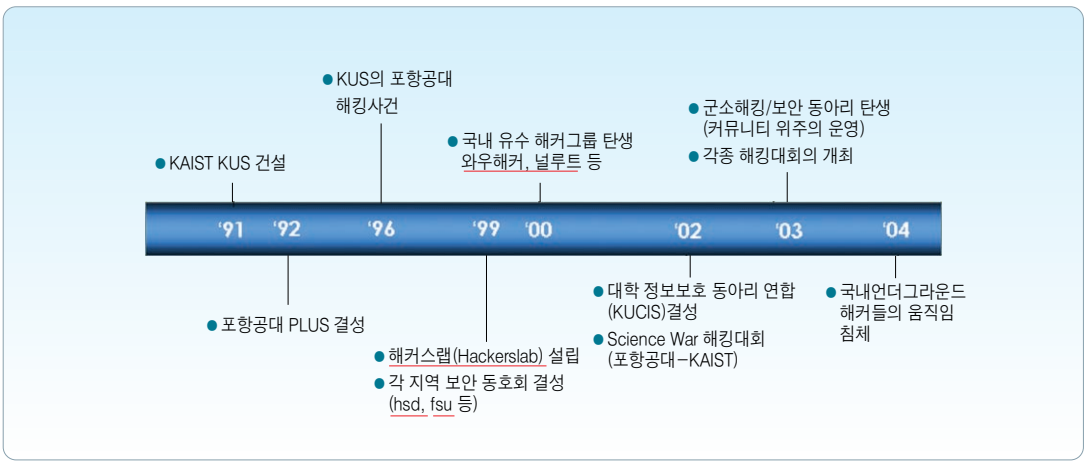
Origin of Digital Attacks, 2003	
Brazil	95,544
Turkey	14,795
USA	2,955
Indonesia	2,360
Egypt	2,365
UK	1,707
Morocco	1,650
Pakistan	1,398
Mexico	1,317
Malaysia	1,215
Source : mi2g	

[그림 4] 공격 근원지 조사 자료

Hacker Capital이라고 불리며 법적으로 해킹에 대한 규제를 하지 않는 브라질을 제외하고는 대다수의 해킹이 미국과 유럽 쪽에서 발생하고 있으며, 최근 들어 중국이 그 대열에 급속도로 합류하고 있음을 또한 확인할 수 있다. 이런 각국에 소속되어 있는 해커들은 그 활동에 있어서 해커들의 연합체인 해커그룹으로 활동하고 있다. 해커그룹들의 전반적인 활동은 외부에 드러나지 않아 유명한 언더그라운드 해커그룹의 경우 소수로 구성되어 자체적인 활동을 하는 경우가 많다고 할 수 있다.

3. 국내 해커그룹 동향

국내의 해커그룹의 역사는 90년대 초반부터 시작되었다고 할 수 있다. 물론 그 전에도 소수의 언더그라운드 해커들에 의한 움직임이 있었겠지만, 일반인들에게 국내 해커와 해커그룹의 존재가 많이 알려지기 시작한 계기는 아마도 카이스트 KUS와 포항공대 PLUS의 해킹 사건일 것이다. 이 사건과 관련하여 1세대 해커들의 움직임에 탄력을 받아서인지 국내 해커그룹은 1999년과 2000년 연이어 해커스랩(hackerslab)의 설립과 각 지역 보안 동호회(HSD, FSU 등)의 활동, 그리고 와우해커(wowhacker), 널루트(null@root) 등의 언더그라운드 해커그룹의 탄생 등 분주한 기간을 보냈다고 할 수 있다. 그 후, 2002년도에는 대학 정보보호 동아리 연합회인 KUCIS가 KISA에 의



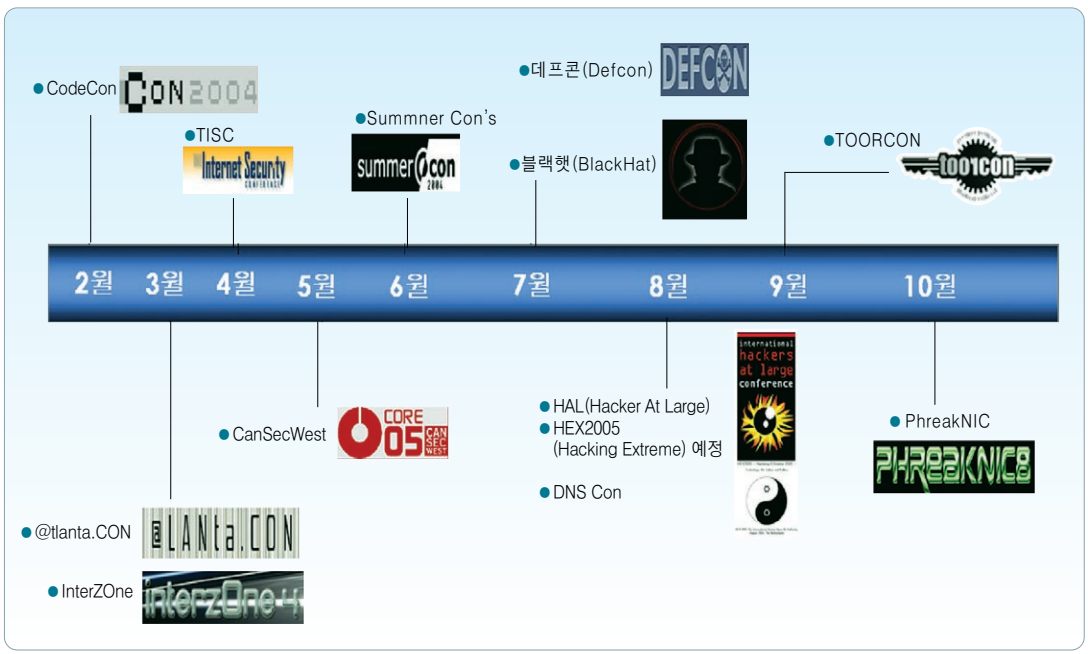
[그림 5] 국내 해커그룹 연대표

해 결성되어 활동을 하였다. 각각의 언더그라운드 해커그룹이나 보안 동호회, 대학 동아리는 현재에도 나름의 기술적인 발전을 위해 연구하고 있고 그 기술력 또한 인정할만한 수준이라고 할 수 있다. 하지만, 이런 각기의 커뮤니티의 결과물이나 파워가 한 곳에 뭉쳐질 만한 계기를 찾지 못했다는 것에서 큰 아쉬움이 남았다고 할 수 있다.

4. 국외 해커그룹 동향 – 컨퍼런스 기반의 활발한 활동

국외 해커그룹의 움직임은 그 활동에서부터 국내와 많은 차이점을 보인다고 할 수 있다. 국내의 경우 정부 기관이나 연구 기관에서 개최하는 여러 형태의 정보보호 관련 행사들이 존재하고 있지만, 보안을 방패에 비유했을 때 창을 위한 즉, 해커를 위한 행사는 없다고 할 수 있다. 국외의 경우 [그림 6]과 같이 다양한 해커그룹들이 모이는 컨퍼런스가 연중 개최되어 기술 교류와 정보 공유의 장으로 활용되고 있다. 특히 데프콘과 블랙햇의 경우 긴 역사를 자랑하고 있어 해당 컨퍼런스를 잘 살펴보면 국외 해커그룹의 활동과 관심사, 기술 동향 등을 쉽게 파악할 수 있다.

국외 해커그룹의 동향을 살펴봄에 있어서 반드시 살펴보아야 할 컨퍼런스가 데프콘과 블랙햇이라고 할 수 있다. 이 두 컨퍼런스에 대한 자세한 내용은 국가사이버안전센터의 'Monthly 사이버 시큐리티' 지난해 8월호에서도 소개한 바 있다.



[그림 6] 주요 컨퍼런스 개최 일정

[그림 7] Black Hat과 DEFCON

5. Hacker Groups...

여러 해커그룹 중, 이미 널리 알려진 해커그룹과 신진 해커그룹 몇 팀을 소개하면, 먼저 cDc(Cult of the Dead Cow)는 백오리피스로 국내에도 많이 알려져 있는 해커그룹이다. cDc는 1984년에 결성되어 활동하여 왔으며, DEFCON 3~9에서의 발표 이외에도 여러 유명 컨퍼런스에 참가하였다. cDc는 백오리피스 이외에도 e-zine과 Hacktivismo, 사이버공간 상에서의 인권과 프라이버시에 대한 주장으로 유명하다고 할 수 있다. cDc 이외에도 DEFCON의 CTF(Capture The Flag) 행사와 관계가 깊은 Ghetto Hackers와 무선과 관계된 해킹/보안 기술을 연구하는 The Shmoo Group 등이 DEFCON에 힘을 실어주는 해커그룹이라고 할 수 있다.

6. Now in Asia-Malaysia, and China

미국과 같은 컨퍼런스 기반의 활발한 해커그룹들의 활동이 아시아에서 없는 것은 아니다. 아시아에

[그림 8] HITBConf2004

[그림 9] HITBConf2004 CTF

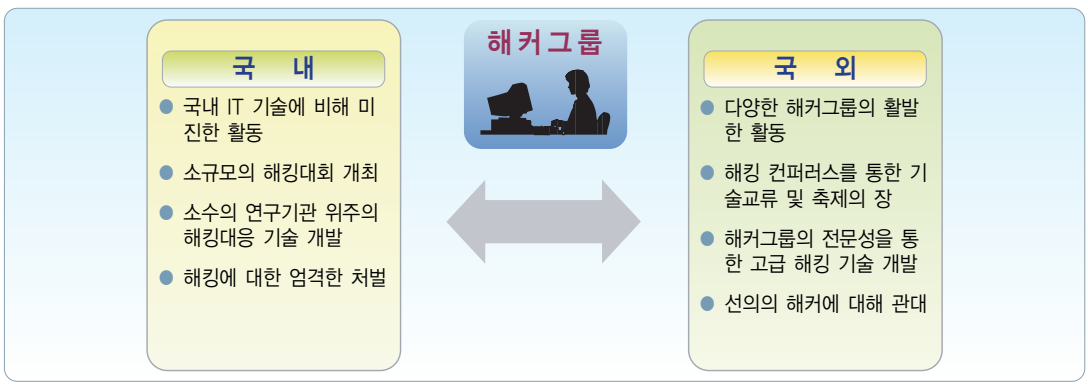
서의 움직임은 말레이시아와 중국에서 찾아볼 수 있다. 말레이시아의 경우 2000년에 창설된 HITB (Hack In The Box)라는 해커그룹에 의해 2003년도부터 Hack In the Box Security Conference가 말레이시아 Kuala Lumpur에서 매년 열리고 있다. 컨퍼런스 준비를 위한 포럼에 등록된 인원이 5천여명에 이르고 Zone-h 등 유명 해커그룹이 참여할 정도로 이미 상당한 인원이 컨퍼런스에 참여하고 있다. 또한, CTF와 브리핑/트래이닝 행사의 구분 등 미국의 블랙햇과 데프콘의 구성을 대부분 수용하여 운영하고 있다는 것이 큰 특징이라고 할 수 있다.

중국의 경우에는 1998년에 Xfocus Team이 주도적으로 Xcon이라는 컨퍼런스를 개최하고 있다. 현재 중국 북경에서 3차례에 걸쳐 행사가 개최되었으며, 자유, 교류, 공존, 창조적 학술 분위기 유지와 보안 기술의 발전을 목표로 행사가 진행되고 있다고 한다.

7. Why not in Korea?

한국에서의 경우, 컨퍼런스 기반의 해커그룹 활동과 기술 교류의 장은 국가 기관이나 대형 정보보호 벤더들에 의해 만들어져 왔다. 외국의 경우가 우리나라와 다르다고 해서 외국의 것이 좋고 전부 받아들이자는 것은 아니다. 한국에는 기술력이 뛰어난 해커그룹이 많고, 또한 제 각기의 노하우를 보유하고 있다. 하지만, 그렇게 자기 자신의 기술을 자기 그룹만이 보유한 채 다른 해커그룹이나 대학 연구기관과의 협력을 통해 여러 형태로의 시너지 효과를 얻지 못하는 경우가 많다.

현재 많은 새로운 기술들과 기법 · 이론들이 발표되고 토론되며, 보안 전문가들이 많은 자료를 참고하고 있다. 이런 상황에서 새로움을 추구할 수 있는 해커그룹의 연구 정신과 실험 정신이 뭉쳐질 수 있는 기회가 있었으면 좋겠다는 생각을 많이 하게 된다. 특히 우리나라와 같은 IT강국에서 컨퍼런스 기반의 해커그룹 활동들이 더욱 공개적이고 역동적으로 이루어지기를 기대해보면서, 국내의 언더그라운드 해커그룹과 대학 해킹/보안 관련 동아리 등의 파워가 한 자리에 모여 '한국 IT 기술의 발전'으로까지 이어지기를 또한 기대해 본다.



[그림 10] 국내외 해커그룹

※ 특별기고는 국가사이버안전센터의 기본입장과 다를 수도 있습니다.