情 報 保 護 學 會 誌
第21卷 第6號, 2011. 10

국가사이버보안정책에서 해킹에 대한 소고

박 대 우*

요 약

7.7 DDoS공격과 3.4DDoS공격, NH금융전산망마비사건, 네이트 해킹 사건 등은 해킹이 개인적 문제를 지나서, 사회와 국가적인 이슈로 부상되고 있다. 중국은 대학에서 해킹 기법을 가르치고, 인민해방군에 국가일꾼이란 소명의식을 주고 있다. 북한은 지도자의 지시로 노동당과 북한군에서 사이버부대를 직접 교육 운영하고 있다. 미국은 외국으로부터 사이버 공격을 당할 경우 이를 '전쟁 행위'로 간주해 미사일 등으로 대응한다는 방침을 세웠다. 이와 같이 해킹은 국가사이버보안 정책에서 다루어져야 할 필요성이 있다. 본 연구에서는 해커의 변천, 해킹기술과 방법, 해킹 툴, 그리고 해킹 사례를 살펴본다. 또한 해킹 동향 분석에서 해킹기술 동향 분석, 해커(사람) 동향 분석, 해킹 지역(국가) 동향 분석을 통하여 해킹 인력의 조직화, 해킹 기술의 집적화, 해킹 조직의 집중화 연구를 한다. 그리고 국가사이버보안정책에서 해킹에 대한 '국가사이버보안법 시행령' 제정, 국가사이버보안 자문회의, 국가사이버보안 협력회의, 해킹 프로세스 전략, 해킹 전략 추진 방법론, 사이버협력국, 해킹 작전국, 인력 양성국, 해킹 기술국에 관한 저자의 개인 의견을 제안한다.

Ⅰ. 서 론

초고속인터넷의 국가간 연결과 개인의 스마트단말기 사용으로 인한 고도지식스마트정보화산업사회에서 정보의 사용량은 급속하게 늘어나고 필요한 정보를 스마트하게 공급하고 있다.

인터넷과 네트워크에서 스마트 정보화 산업의 발달과 함께 침해사고도 늘어나고 있으며, 침해사고의 원인을 제공하고 있는 해킹(Hacking)은 기술적으로 진화되면서 사회적 국가적 문제로 대두되고 있다.

2009년 7.7 DDoS공격(Distributed Denial of Service공격)과 2011년 3.4DDoS공격, NH 금융전산망 마비사건, 네이트 해킹 사건 등은 국민의 우려와 관심을 반영하면서, 신문과 방송의 헤드라인 뉴스로 발표되고 있다. 즉 해킹은 개인적인 문제를 지나서, 사회와 국가적인 이슈로 부상되고 있다.

공산국가인 중국은 인민해방군이 해커들을 조직화하고 청두기술대학 등 대학에서 프로그램(해킹 기법)을 가르치기 시작하면서 국가를 위해 일하는 '국가일꾼(State Actor)'이란 소명의식으로 보편화하였다[1].

북한의 지도자인 김정일은 2007년 3월 평양시 근교의 한 공장을 시찰하면서 "현대전은 전자전이다. 적의 전자전 능력을 마비시킬 수 있는 전술을 개발하라"고 지시하였다. 5년제 대학에서 매년 100여 명의 컴퓨터 전문가를 키우고, 이와 더불어 컴퓨터과학 전공자를 합쳐 정예 150여 명을 추린 다음, 기본교육 1년을 마치면 군관(장교)으로 임관된다고 한다. 이후 정찰총국이 직할 운영하는 압록강군사대학으로 보내 '사이버전사'로 양성한다[2].

이에 대항하는 자유민주국가인 미국은 외국으로부터 사이버 공격을 당할 경우 이를 '전쟁 행위'로 간주해 미사일 등으로 대응한다는 방침으로 사이버국방(WAR)의 전략을 세웠다. 영국은 현역 장성을 사이버전 사령관으로 임명하고 공격형 사이버 기술을 개발하고 있다.

이와 같이 해킹은 국가 사이버 보안 정책에서 다루어져야 할 필요성이 있다.

본 연구에서는 해커의 변천, 해킹기술과 방법, 해킹 툴, 그리고 해킹 사례를 살펴본다. 또한 해킹 동향 분석에서 해킹기술 동향 분석, 해커(사람) 동향 분석, 해킹 지역(국가) 동향 분석을 통하여 해킹 인력의 조직화, 해킹 기술의 집적화, 해킹 조직의 집중화 연구를 한다. 그리고 국가사이버보안정책 연구에서 해킹에 대한 소고를 추출한다.

* 호서대학교 벤처전문대학원 IT응용기술학과 교수(prof1@paran.com)

Ⅱ. 관련연구

2.1 국내 2011년 침해사고 현황

다음은 한국인터넷진흥원(KISA)의 2011년 월간 침해사고 전체 통계이다[3].

■ 침해사고 통계 요약

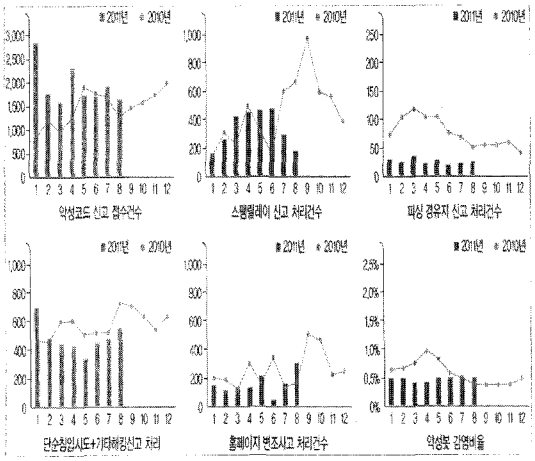
- 2011년 8월 악성코드 신고건수는 총 1,695건으로 전월(1,912건) 대비 11.3% 감소하였으며, Agent(222건), OnlineGame Hack(181건), OnlineGame-Hack69(92건), Winsoft(82건) 등의 순으로 많이 접수되었다.
- 2011년 8월 해킹신고 처리건수는 총 1,115건으로 전월(956건)대비 16.6% 증가하였고, 스팸릴레이를 제외한 피싱경유지, 단순침입시도, 기타해킹, 홈페이지변조 등은 모두 증가추세를 보이고 있다.

■ 침해사고 위협 분석 요약

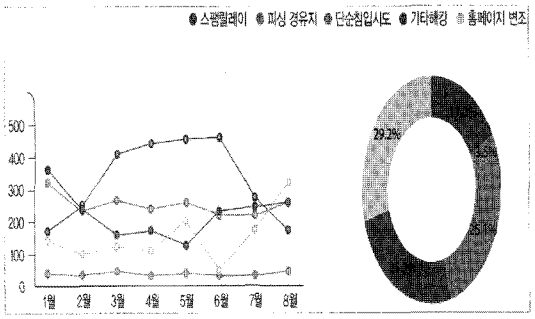
- 악성코드 유포 및 경유사이트는 총 898건으로 전월(1,589건) 대비 43.5% 감소하고 있으며, 기관유형별로는 기업(86.3%), 웹서버 유형별로는 MS-IIS(66.4%)가 가장 많은 비율을 차지한다.
- KISC 허니넷으로 유입된 전체 유해 트래픽은 약 622만건으로 전월(664만건) 대비 6.3% 감소하였다.
- 사고 유형별 증감추이를 살펴보면, 2011년 7월 대비 피싱경유지(25.8%), 단순침입시도 (25.0%), 기타해킹(14.7%), 홈페이지 변조(77.2%) 등은 증가하였고, 스팸릴레이(30.5%)만 감소하였다. 또한 스팸릴레이 유형은 연중 최고치를 기록했던 6월 이후 큰 폭의 감소가 이어졌고, 홈페이지 변조 유형은 6월 최저치 이후 큰 폭의 증가추세가 이어지고 있다.

구분	2010년 총계	2011년												2011년 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
악성코드	17,930	2,920	1,847	1,566	2,335	1,786	1,763	1,912	1,695					15,824
해킹신고처리	16,295	1,025	864	1,002	999	1,091	957	956	1,115					7,969
· 스팸릴레이	5,216	174	266	408	443	448	453	272	189					2,643
· 피싱 경유지	891	30	25	38	24	29	22	31	39					238
· 단순침입시도	4,126	322	231	272	243	257	214	224	280					2,043
· 기타해킹	3,019	558	239	155	179	121	222	245	281					1,800
· 홈페이지 변조	3,043	141	103	129	110	206	46	164	326					1,245
악성놈(Bot)	0.6%	0.5%	0.5%	0.4%	0.4%	0.5%	0.5%	0.5%	0.5%					0.5%

〔그림 1〕 KISA 2011년 월간 침해사고 전체 통계



〔그림 2〕 KISA 2011년 월별 침해사고 전체 통계 그래프



〔그림 3〕 KISA 유형별 증감추이 및 비율

- 사고 유형별 비율을 살펴보면, 홈페이지 변조(29.2%), 기타해킹(25.2%), 단순침입시도(25.1%), 스팸릴레이(17.0%), 피싱경유지(3.5%) 순으로 나타났다.

Ⅲ. 해킹과 해커의 변천 분석

3.1 해킹, 해커의 정의와 해커의 변천

■ 해킹, 해커, 해킹 공격의 정의

해킹은 네트워크에 연결되어 있는 컴퓨터에 불법적인 침입을 하는 것으로, 허가받은 범위를 벗어나서 컴퓨터 내의 자원에 대한 접근을 하는 것을 말한다.

크래킹(Cracking)은 컴퓨터에 침입해 들어가, 고의적으로 경제적인 이득을 취하거나 하드웨어를 마비시키고 소프트웨어를 훔치거나 데이터를 파괴하는 행위를 말한다.

하지만 현재 해킹의 의미는 이 두 가지를 포함하는 포

괄적인 의미로 사용되고 있으며, 해킹을 통해 침해사고를 유발을 목적으로 하는 행위는 해킹 공격이라고 한다.

해킹을 하는 사람을 해커(Hacker)라고 한다. 해커는 화이트햇 해커(White-hat Hacker), 블랙햇 해커(Black-hat Hacker)로 분류되고 있다. 화이트햇 해커는 모의 해킹(Penetration Testing)이나 취약점 점검 등의 해킹 기법을 사용하는 전문적인 보안전문가를 말하며, 한국에서는 화이트 해커라고도 한다. 블랙햇 해커(Black-hat Hacker)는 해킹에 대한 자기만족이나, 공익의 관점이라고 생각하면서 해킹을 시도한다.

하지만 허가받은 범위를 벗어나서 개인과 사회와 국가에 대한 컴퓨터와 네트워크에 대한 침해사고를 발생시키는 행위의 주체가 해커이며, 타인에게 의도적으로 피해를 발생시킨다면 법적인 책임을 져야 한다.

■ 해킹하는 해커의 레벨

해커가 하는 해킹의 레벨은 학술적이나, 법적으로 근거는 없으나, 해커 매니아들이 일반적으로 분류하는 해킹의 레벨은 레이머 -> 스크립트 키드 -> 디벨롭 키드 -> 크래커 등으로 나눈다.

레이머(Lamer)는 해커가 되고 싶지만 네트워크와 운영체제에 대한 지식도 많지 않다. 컴퓨터를 단순히 게임과 채팅, 인터넷에서 와레즈 사이트 찾기 등에 사용하면서 와레즈 사이트에서 트로이안 목마 프로그램이나 DoS 공격 툴 등의 해킹 툴을 내려 받아 이용하면서 해커인 것처럼 생각한다.

스크립트 키디(Script Kiddie)는 네트워크와 운영체제에 대한 약간의 기술적인 지식을 갖고 있는 해커들이다. GUI 환경의 운영체제에만 익숙하며, 공격 기법도 기존에 잘 알려진 툴을 이용하여 인터넷 사용자를 괴롭히는 일을 한다.

디벨롭트 키디(Developed Kiddie) 해커는 대부분의 해킹 기법을 알고 있다. 해킹 수행 코드가 적용될 수 있는 취약점을 발견할 때까지 여러 번 시도해 시스템 침투에 성공할 수 있는 해커들이다.

구루 익스페리언스드 테크니션(Guru Experienced Technician), 세미 엘리트(Semi Elite)로 구분되는 해커는 컴퓨터에 대한 포괄적인 지식이 있고 운영체제와 네트워크에 대한 지식도 갖추고 있으며, 운영체제에 존재하는 특정 취약점을 알고 이 취약점을 공격할 수 있는 해킹 코드를 만들 수 있다. 또한 타인이 만든 해킹 프로그램을 사용하지만 프로그램을 수정해서 자신이 원하는 목표 작업을 할 수가 있다. 하지만 해킹 흔적을 완벽하게 지우지 못해 추적당할 수 있다.

위저드 엑스퍼트(Wizard Expert), 엘리트(Elite) 로 구분되는 해커는 컴퓨터, 네트워크, 운영체제, 프로그래밍 등 컴퓨터에 대한 포괄적인 지식을 갖추고 있으며, 해킹하고자 하는 시스템의 새로운 취약점을 찾아내어 해킹할 수 있는 최고 수준의 해커이다. 또한 해킹을 한 후 흔적을 완벽하게 지울 수 있어 추적하기 힘들다.화이트 위저드는 대부분 대학에서 공부를 하고 학문적인 접근을 하여 방어 프로그램인 네트워크 보안, 방화벽, IDS, IPS 등을 만들거나, CERT/CC에 근무를 한다. 다크 위저드는 마니아 또는 오타쿠라고 불리면서 유명대학 학벌보다는 독학이나, 네트워크 그룹활동으로 해킹 공격을 하고 목적을 달성하는 경우가 많다.

이외에도 인터넷의 분류에는 위저드 네메시스(Wizard Nemesis)라는 명명된 세계 최고 등급의 해커로 구분된다. 지금까지 네메시스 등급으로 기록된 해커는 10명이 미만으로 실명이 밝혀진 사람도 2명이 있으며, 생사 불문하고 잡아오면 몇 십억원의 상금이 걸린 3명도 있다. 또 위저드 킹(Wizard King)은 해커가 궁극적으로 지향하는 단계로 컴퓨터 하드웨어, 운영체제, DB, 보안, 통신, 네트워크, 통신보안 등 모든 분야에 있어서 완벽한 이해를 가지고 있는 사람이다. 리누스 토발즈(Linus Benedict Torvalds)가 명예 위저드 킹으로 추대된 적이 있었지만 스스로 고사하였다.

3.2 해킹 방법과 기술 변천

■ 해킹 방법의 변천

해킹 방법의 변천은 컴퓨터와 네트워크 기술의 발달과 더불어 다양하게 불규칙적으로 나타나지만, 일반적으로 정보 수집 단계와 의도적인 접속 단계, 해킹공격 단계, 역추적 배제 단계, 사회공학적 공격 단계 등의 해킹 방법들이 사용되어 졌다.

정보 수집 단계의 출발은 정보 수집으로 살라미(Salami)로 조금 씩 정보를 모으는 것으로 시작한다. 다음 쓰레기 모으기(Scven)로 휴지통 뒤지기 등 이다.

의도적인 접속 단계의 Packet Sniffing은 네트워크 상에서 공격 목표의 패킷을 분석하여 내용을 볼 수 있다. 공격 목표가 설정되면 슈퍼 재핑(Super Zapping)으로 보안을 무력화 시키는 관리자 패스워드 탈취나, 백도어 프로그램을 이용하여 해킹한다.

해킹 공격 단계의 IP Spoofing 공격은 IP Address를 의도적으로 조작하여 관리자인 것처럼 침투하는 것이며, 버퍼 오버플로우(Buffer Overflow) 또는 버퍼 오버런(Buffer Overrun)은 메모리를 다루는 데에 오류가 발생하여 잘못된 동작을 하는 프로그램의 취약점을 이용하여, 입력의 경계를 넘어서 리턴주소를 바꾸어 공격한다. FSB(Format String Bug)는 출력 문에서 올바르지 못한 방법을 악용하여 공격 목표의 포맷인자를 이용하여 출력 포인터를 바꾸어 공격한다. 또한 Injection공격은 SQL Injection 취약점과 같이 공격의 결과가 서버의 장악이나 데이터베이스 손상이 발생하게 한다.

역추적 배제 단계로 XSS(Cross-Site Script) 공격은 실제로 취약점이 있는 웹서버를 공격하는 것이 아니라, 제 3자를 공격하는 공격 경유지 성격을 띠고 있다. XSS 취약점을 이용하여 공격자는 웹 애플리케이션에 접근하는 다른 사용자에게 자바스크립트를 실행할 수 있게끔 허용함으로써 공격이 시작된다. XSS 공격의 예로 악성 스크립트와 XSS 공격을 합쳐서 타인의 계정 정보를 빼내어, 공격자가 피해자의 정보를 도용하여 로그온 할 수 있게 된다.

사회공학적 공격 단계인 피싱(Phishing) 공격은 일반적으로 위조된 웹사이트를 통해 누군가가 다른 사람을 사칭하여 개인정보 또는 기타 민감한 정보를 공유하도록 속이는 수법을 말한다. 악성코드는 소유자가 알지 못하는 사이에 컴퓨터에 설치되는 소프트웨어로서 컴퓨터를 손상시키거나 정보를 도용하는 것을 목적으로 한다. 파밍(Pharming) 공격은 DNS 데이터를 위변조하여 공격하며 DNS 캐시 포이즈닝(DNS Cache Poisoning)이라고도 한다. 온라인 뱅킹 서비스를 이용하기 위해 은행 웹 사이트 www.abank.co.kr에 접속하는 경우에, 진짜 주소는 201.12.345.6이지만, 악의의 공격자는 www.abank.co.kr의 주소를 위변조하여 침해사고를 유발하여 금융의 피해를 유발 할 수 있다.

■ 해킹 방법 내용의 변천

해킹 방법 내용의 변천은 자료를 위변조하는 공격과 비동기성 공격으로 CPU와 입출력 장치의 속도 차를 이용하여 공격하는 방법, 포트 스캔으로 침투하기 위한 네트워크에서 포트를 검색하여 공격의 채널을 확보하는 방법 등이 있다.

암호 해독 방법은 암호 해독 소프트웨어를 사용하여 암호 파일을 해독하여 침투하는 것이다.

트로이 목마(Trojan Horse)는 일반 프로그램을 악의적으로 변경시킨 후 침투시켜서, 프로그램이 작동하면 컴퓨터 사용자도 모르게 정보를 빼내거나, 사용자가 키보드로 입력하는 모든 정보를 알아낼 수 있다.

스푸핑(Spoofing)은 허가 받지 않은 사람이 마치 신뢰성 있는 사람이 네트워크를 통해 데이터를 보낸 것처럼 네트워크 상의 데이터를 변조하여 접속을 시도하는 침입 형태이다.

스니퍼(Sniffer)는 네트워크상에서 전송중인 데이터를 가로채는 프로그램이다.

위장 채널(Covert Channel)은 컴퓨터 시스템의 내부 특성을 이용하여 불법적으로 네트워크를 이용한 통신 채널을 생성시켜 정보를 유출 시킨다.

또한 네트워크의 가용성을 마비시켜 업무를 마비시키는 서비스 거부공격(Denial of Service)과 사용자에게 스팸(Spam) 메일을 전송해 목적을 이루기도 한다.

현재 가장 급속하게 발전하는 스마트폰에 대한 공격의 내용은 다음과 같다.

Platform 공격은 스마트폰 OS 및 플랫폼 상의 취약점 혹은 고유의 기능적 특징으로 인한 파생 공격을 하여 바이러스 및 악성코드, 키보드 해킹, SMS 후킹, 프로세스 및 메모리(덤프)를 해킹할 수 있다.

Application 공격은 바이러스와는 달리 사용자가 인지하고 있는 실행 애플리케이션에 의한 공격으로 피싱 프로그램, 데이터 파일 및 실행 파일 변조, 역공학, DoS 및 DDoS공격이 있다.

Storage 공격은 스마트폰에 내장 /외장 메모리에 탑재된 파일시스템 접근 및 기밀정보 추출 공격하는 것이다. 또한 스마트폰 내부 스토리지 파일 시스템 접근 및 추출, 활성 데이터 및 삭제된 기밀정보 추출도 있다.

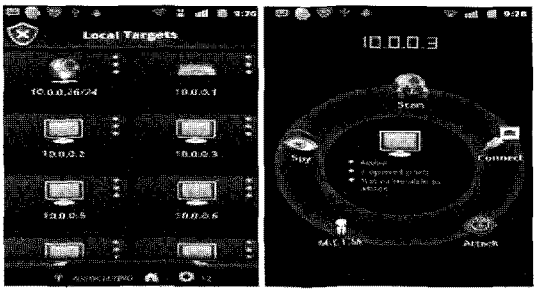
3.3 해킹 공격 툴

해킹 공격을 하는 해커는 목적을 달성하기 위해 해킹 툴이나 해킹 스크립터 등을 사용한다.

최근 스마트폰에 대한 해킹 툴로는 @ihackbanme로 알려진 잇자크 주크 아브라함은 데프콘에서 새로운 해킹 툴을 선보였다. 짧게 'Anti'로 불리는 '안드로이드 네트워크 툴킷'이다.

다음은 해킹 툴에 관한 내용이다.

▲ 암호 크랙 : advanced ZIP password recovery 3.54, elcom soft



〔그림 4〕 안드로이드 해킹 툴 'Anti'

▲ 익명 메일 : anoy mail
▲ 프록시서버
▲ 논리폭탄
▲ 폭탄메일 : kaboom v3.0
▲ 게시판 광고글 : ad-smashing
▲ 패스워드 크랙 : iopus password recovery, revelation, snadboy's
▲ 날짜제한 크랙 : data cracker
▲ Virus 만드는 툴 : nuke randomic life generator
▲ 주민번호 생성기
▲ 신용카드번호 생성기
▲ 휴대폰 문자 공짜 보내기 : 간딴 문자 v1.7
▲ 버그공략 툴 : exploit
▲ 사전파일 생성기 : password generator
▲ 웹 사이트 크래킹 : wwwhack, web cracker, golden eye, meteor swarm
▲ 키보드 입력 크래킹 : iks (process -> log.exe), ghost keylogger (process -> syncconfig.exe), sc-keylog2 (process -> hacker.exe), 마우스 로거
▲ 프로그램에 lock거는 프로그램 : program lock, mouse trap
▲ 파일과 문서에 암호화 하는 프로그램 : file safe
▲ 패스워드 생성기 : chaos generator, advanced password genarator
▲ 패스워드 관리 프로그램 : 알패스, key pack2000, mypassword
▲ 트로이 목마 프로그램 : netbus 2.1, netbus 1.7 (강력함), 백오리피스 2000, sub seven 2.1, haktek 1.1, gaban bus2
▲ 파일합치는 프로그램 : senna spy one exe hacker 2000
▲ 트로이 목마 제거 툴 : tavscan, the cleaner
▲ 개인방화벽으로 유명한 보안 프로그램 : 존 알람, 누구야? 피시(국내), 데프콘(국내), 블랙아이스 디펜더
▲ IP 추적기 프로그램 : visual route, neo trace express
▲ 원격제어 프로그램 : remote administrator
▲ 온라인게임 크래킹 제거 전문 툴 : dkremover
▲ MSN에 폭탄메세지 보내는 프로그램 : wolfpack MSN bomber
▲ ICQ에 폭탄메세지 보내는 프로그램 : ICQ boomber
▲ IP주소 이용한 메세지 발송 프로그램 : speed marketer
▲ 해킹기법 실시간 배우는 : security monitor
▲ 프록시 서버 검색 마법사 : proxy hunter
▲ 웹사이트 조회수 조작 프로그램 : m3hm3t's clicker
▲ 홈페이지 소스 암호화 : web protector
▲ 엡서버의 인증 크랙하기 : obiwan
▲ 파일다운로드할때 바이러스 차단하기 : vcatch
▲ 네트워그 상의 IP주소 스캔하기 : ANGRY IP SCANNER
▲ 해킹 시뮬레이션 게임 프로그램 : hacker
▲ 키로거 : 사용자의 입력값을 수집해 등록된 이메일 주소로 보내는 기능.

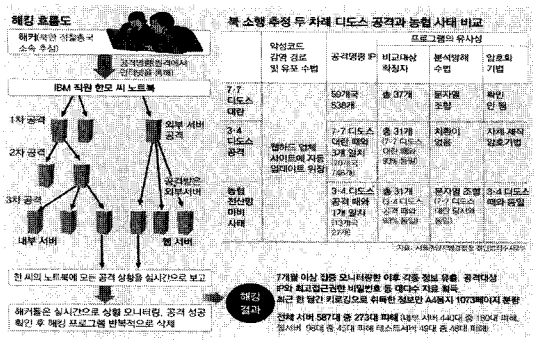
3.4 해킹 공격 사례

최근해킹 공격 사례를 중심으로 주요 해킹 공격 사례를 설명한다.

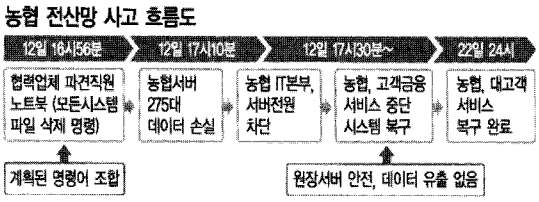
■ NH 서버 해킹 금융전산망 마비 사례

서울중앙지검 첨단범죄수사2부(부장검사 김영대)는 2011년 4월 12일 발생한 NH 금융전산망 마비 사태에 대해 "북한이 7개월여에 걸쳐 치밀하게 범행을 준비하고 실행한 새로운 차원의 '사이버 공격'"이라고 밝혔다. 검찰은 국가정보원 등 유관기관과 공조수사를 벌인 결과 북한 군부에서 대남테러와 해외공작을 전담하는 '정찰총국'이 원격조종으로 농협 전산망을 파괴한 것으로 최종 결론을 내렸다고 한다[4].

검찰은 2010년 9월 삭제명령이 내려진 것으로 추정되는 노트북이 좀비PC가 되었으며, 범인들은 7개월 이



〔그림 5〕 NH 해킹 비교(검찰 발표 참조)

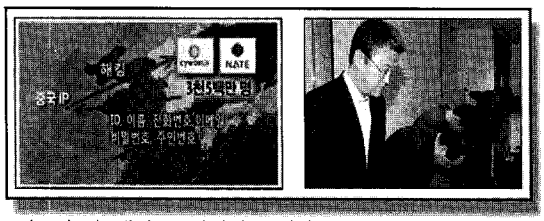


〔그림 6〕 NH 금융전산망 해킹사고 흐름도

상 노트북을 집중 관리하면서 필요한 정보를 획득한 뒤 원격 조종으로 공격했다고 발표했다. 좀비PC 노트북에 숨어 있던 악성코드 81개 암호화 방식이 2009년 7월7일과 2011년 3월4일 DDoS 공격과 비슷하고, 컴퓨터 조종에 이용된 IP 1개가 3월4일 DDoS 공격 때와 완전히 일치한다는 사실을 들어 북한의 소행으로 최종 결론을 냈다. 검찰은 또 악성코드를 운영하기 위한 백도어 기능과 좀비에 명령을 내리는 서버목록이 1개의 프로그램이 아니라 별도 파일로 제작된 점 등이 DDoS 공격 사건과 매우 유사하다는 이유를 정황 증거로 제시했다.

NH 서버 해킹사건으로 NH금융전산망과 업무가 마비됐다. 해킹은 금융 백업서버까지 동시에 이뤄졌다.

좀비PC로 부터의 역추적 흔적을 없애기 위해 한 특정 파일을 수차례 지운 흔적, 그리고 그 파일을 지운 접속기록인 로그를 삭제한 흔적이 있으며, 수백 대의 서버를 동시에 해킹한 이유는 역추적 시간을 벌기 위해서였을 가능성이 높아 보인다.



〔그림 7〕 네이트, 사이월드 해킹으로 인한 회사측 사과

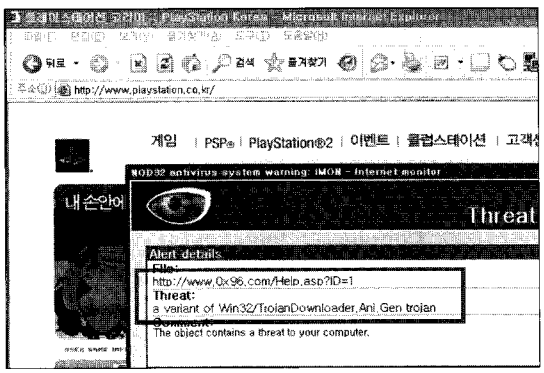
■ NATE와 싸이월드 해킹 사례

3,500만명의 NATE 메일 사용자와 2,500만명의 싸이월드 사용자가 해킹 당하였다.

해킹으로 인하여, 아이디는 물론이고, 비밀번호, 이름, 전화번호, 주민등록번호, 주소, 이메일주소까지 개인정보가 유출되었다고 한다. 특히 개인정보 유출은 스팸메일이나 보이스피싱, 금융범죄 등으로 악용될 수 있어, 비밀번호 변경 등 즉각적인 정보보호 조치가 필요하다.

■ SONY 플레이스테이션 홈페이지 해킹 사례

2011년 4월 해외 SONY 플레이스테이션 네트워크를 해킹 당해 약 7천700만명의 고객 개인정보를 유출 당한 것을 시작으로 5월과 6월에도 잇따라 해킹을 당하여 약 20여 차례 해킹을 당한 바 있다.



〔그림 8〕 홈페이지 해킹 후 악성 코드 배포 중

〔그림 9〕 홈페이지 2차 해킹 후 악성 코드 배포 중

IV. 해킹 동향 분석

4.1 해킹 동향 분석

2009년 7.7 DDoS 공격과 2011년 3.4 DDoS 공격 및 NH 서버 해킹 금융전산망 마비 사태에서 국민들은 해킹에 대한 사회적 피해를 인식하고 국가 차원의 사이버보안정책의 필요성이 요구 되고 있다. 이러한 요구의 기초자료로서 최근의 해킹 사례를 중심으로 해킹 동향 분석을 해 본다.

■ 2010년 12대 보안침해사고 해킹 위협

① DDoS 공격용 좀비 PC 확보 기법 지능화

7.7DDoS 공격 이후, 대량의 좀비 PC를 확보하여 공격이 증가하였다. 다수의 좀비 PC를 이용해 공격하여 금전적 대가를 요구하고 확보한 좀비 PC 자체를 거래하는 시장이 활성화되었다. 또, C&C(Command & Control) 서버를 통해 지속적으로 좀비 PC의 악성코드를 업데이트하고, 능동적 공격정보를 생성하고 있다.

② 스마트 폰 공격 위협 본격화

2009년 11월 아이폰의 국내출시로 본격적인 스마트폰 시대가 되었고 PC에서 발생한 보안문제가 스마트폰에서도 발생이 가능하게 되었다. Jail Break(탈옥)된 아이폰에 악성코드가 발견되었고 통화기록이나 전화번호, 사진 등을 탈취하고 스마트폰이 DDoS공격의 좀비 Client로 악용되어 비정상적인 트래픽을 유발해 불법과금이 발생하거나, 배터리의 소진 공격을 한다.

③ 클라우드, 가상화 기술 악용한 보안 위협 증가

클라우드와 가상화 기술로 IT 자원 활용의 효율화를 위한 기술로 사이버 공격에 클라우드, 가상화 기술로 악용이 가능하다. 여러 대의 C&C 서버를 하나의 가상화 사설 서버를 사용하여 저렴한 비용으로 봇넷의 구축이 가능하다.

④ 웹 사이트와 스팸 메일이 결합한 위협 증가

2010년에도 웹사이트가 악성코드 전파의 주요경로로 이용되었다. SQL 인젝션, XSS 등 사이트 취약점을 이용하여 악성코드를 전파하고 스팸 메일과 웹 사이트가 결합된 보안 위협이 증가하였다. 이메일을 이용하여 악의적인 웹사이트로 유도하거나 유도 후 웹 브라우저의 취약점 공격하여 악성코드를 설치하는 공격을 하였다.

⑤ SNS를 이용한 공격 확산

2010년 트위터, 페이스북과 같은 SNS를 대상으로한 해킹의 증가로 트위터에 짧은 주소 서비스 이용하여 악성코드를 유포하는 사례가 발생하였다. 스마트폰의 급속한 보급으로 다양한 SNS 애플리케이션이 등장하였고 개인정보를 노린 해킹이 확산되었다.

⑥ VoIP(Voice over Internet Protocol) 보안 위협

VoIP의 보급 확산으로 보안 위협도 함께 증가하였고 특정 VoIP 서비스의 통화 내용을 유출하는 악성코드가 발견되었다. VoIP의 도감청의 위협 증가로 무선 인터넷 공유기의 ID와 비밀번호를 탈취하거나 악성코드를 설치하여 개인 정보 유출의 피해가 증가되었다.

⑦ 메신저 피싱 급증

메신저 프로그램의 편리성을 이용한 악의적 행위가 발생하여 악성코드의 유포 및 금전적 사기가 지속되어지고 인터넷 포털에서 SNS까지 동일한 계정을 사용할 경우 2차, 3차의 피해가 발생 하고 있다.

⑧ 악성코드의 자기 보호 기법 지능화

보안 SW가 접근하지 않는 영역에서 활동하는 악성코드가 발생하고 있다. 은폐 및 자기 보호 기법을 보유한 악성코드가 급증하고 단순 파일 삭제만으로는 치료가 되지 않도록 지능화되어지고 있다. 진단과 치료 기술은 더 복잡해지고 시간과 노력이 더 필요하다.

⑨ 윈도우 7 취약점 공격 증가

2009년 10월 윈도우 7 발표 후 보안 취약점이 발견되어 윈도우 7에 대한 악성코드 제작자의 공격이 증가하고 주요 애플리케이션(MS 오피스, 어도비 PDF 등)에 대한 취약점 공격도 지속적으로 일어나고 있다.

⑩ 사회공학기법의 정교화

사회공학기법에 기반한 악성코드의 증가로 페이스북과 트위터 등 SNS 기반으로 증가하고 인터넷 검색 결과를 인위적으로 조작하는 정교한 기술인 SEO (Search Engine Optimization) 공격까지 등장하였다.

⑪ 가짜 백신 확산

가짜 백신이 2009년에 이어 지속적으로 확산되어 '악성코드에 감염되었다'는 허위 문구를 이용하여 결제를 유도하고 있고, 현재 무료 백신이 개인 시장에 대량 제공되고 있으나, 일부 고객은 지속적으로 가짜 백신에 비용을 결제하고 있다.

⑫ 온라인 게임 해킹 증가

2009년에 이어 온라인 게임의 성장으로 게임에 대한 해킹 역시 증가하고 있다. 메모리 해킹과 오토플레이가 급증하고 온라인 게임 종류(캐주얼 게임, 기능성 게임 등)의 다양화로 해킹 또한 다양화되어지고 있다.

■ 모바일 단말기 해킹과 콘텐츠 해킹

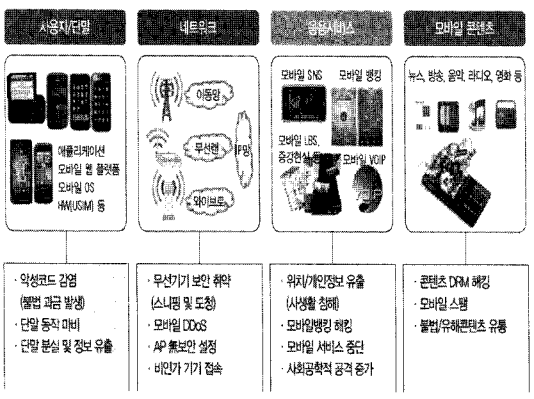
스마트폰 사용자가 2천만명에 육박하고 있다. 엔드포인트 보안인 스마트폰 등에 대한 모바일 해킹이 증가되고 있다. 모바일 인터넷 환경에서도 인터넷 침해공격, 바이러스·웜 감염, 정보유출 등 기존의 보안 위협이 재현될 수 있다. 해외 모바일 악성코드 유포 사례를 통해 유추해 볼 때 국내의 경우도 2011년 하반기부터 금전적 이득을 노리는 스마트폰 악성코드의 출현이 예상되고 2012년부터 본격적으로 악성코드가 유포될 것으로 전망된다.

2010년 4월, 윈도 모바일 운영체제를 사용하는 스마트폰을 대상으로 국제전화 무단발신을 유발하는 모바일 악성코드가 국내에서 처음 발견되었으나, '스마트폰 정보보호 민·관 합동대응반'의 사전조치 및 신속한 대응하였던 사례가 있다.

또한, 스마트폰 및 모바일 단말에 무선랜(Wi-Fi), 블루투스, 이동통신서비스(3G, 4G), GPS통신 등 복수의 통신기능이 기본 탑재됨에 따라 침해경로가 다변화되고 있으며, 모바일 단말을 이용한 IPTV(Internet Protocol Television), 클라우드 컴퓨팅 등 신규 서비스가 무선 환경으로 이용됨에 따라 안전성을 위협하는 요인도 증가하고 있다.

또한 중요한 개인정보를 담고 있는 모바일 단말의 분실·도난 시 개인정보 노출, 사기범죄에 악용 등의 피해가 우려되고 스마트폰을 변형한 Jailbreak, Rooting을 할 경우 해킹에 노출될 위험성도 크다.

또한 위치기반 서비스(LBS)에 의한 개인 위치 노출 및 사생활 침해 가능성이 긴급구제서비스 범위와 상충되는 내용이 있다.



〔그림 10〕 모바일 단말의 4대 영역별 보안위협

모바일 단말기를 통한 콘텐츠에 대한 사용자 등급의 제한을 벗어난 불건전 정보 접근 및 전달과 유해 사이트 접근의 위험성도 우려되고 있다.

■ 국가 인프라 및 제어 시스템에 대한 해킹 위협

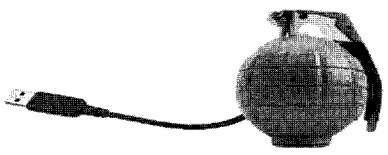
국가의 인프라를 구성하고 있는 국방망, 행정망, 전력, 항공, 수자원 시스템 등과 같은 주요 핵심 인프라에 대한 공격이 사이버국방에 관한 비대칭전력으로서 국가안보에 중대 영향을 주고자 하는 사이버 해킹 공격의 주요 목표가 될 수 있다.

2007년 에스토니아 정부 사이트가 3주간 공격을 받는 일이 발생하자 에스토니아는 당시 마찰을 빚고 있던 러시아를 국가사이버해킹의 배후로 지목했다. 2008년에는 러시아와 그루지아의 해킹이 국가간에 이용된 것을 분석된다. 2008년 미국 국방부에 대한 해킹 공격으로부터 2009년이 미국 연방항공국 네트워크에 대한 해킹 공격과 미국 전력망에 대한 해킹 공격이 이루워 졌다.

개인의 해킹에서 국가의 해킹으로 변화된 것의 표면적인 원인은 2010년 국가 기간시설을 파괴할 목적으로 제작된 신종 악성코드인 '스텍스넷(Stuxnet)'의 등장이다.

'스텍스넷'은 국가 주요 기반시설의 제어 시스템을 공격, 파괴하는 최초의 악성코드로 전산망에 침투해 통합제어시스템에 오작동을 일으켜 시스템을 마비시킨 사이버 무기다. 스텍스넷은 6개월간 7,300여대 감염(2011. 1. 11 전자신문)시켜서 사이버무기로서의 공격을 알렸다. 악성코드의 무기는 이란 원자력발전소의 원심분리기 중 1,000여대를 가동 중단시킨 바 있다. 당시 외신들은 "이스라엘 등이 해킹의 배후에 있었을 것"으로 추측했다. 악성코드가 매우 치밀하게 짜여 있어 국가적인 지원 없이는 해킹 공격을 위한 악성코드 제작이 힘들 것이란 이유에서다.

국가 인프라에 대한 사이버 공격은 해킹이나 바이러스를 이용하여 감염시키고, 피싱 등의 기법으로 컴퓨터 시스템과 통신망 등에 침입하여 네트워크와 서버 등의



〔그림 11〕 미국-이스라엘, 이란 핵시설 스텍스넷 공격 (2011. 1. 16 아시아투데이)

제어시스템을 마비시키는 것이다. 대표적인 공격 수단인 해킹에는 DDoS공격, 멀웨어, 컴퓨터 바이러스, 웜, 전자 폭탄 등 여러 가지 수단을 썩어서 사용한다.

스카다(SCADA : Supervisory Control And Data Acquisition)는 사회기반 사업 시설을 제어하기 위한 시스템으로 스턱스넷 악성 코드와 같은 악의적인 해킹 공격자에 의해 사이버 테러를 당할 경우 통신, 수력, 화력, 전력, 건설, 자동차, 에너지 시설에 대한 직접적인 국가 피해뿐만 아니라, 국민의 인명피해를 통한 국가 안보에 영향을 미친다.

■ 금융 네트워크와 금융 관련 업무 해킹

미국의 코어플러드는 대규모의 금융 데이터를 수집이 가능하며, 금융 데이터를 수집 후에는 자기가 원하는 정보를 다시 뽑아 낼 수 있다.

미국 FBI는 2011년 5월 11일 코어플러드(Coreflood) 멀웨어에 감염된 컴퓨터를 가지고 있는 사용자를 대상으로 봇넷 컴퓨터에 멀웨어를 제거하기 위해 서면으로 동의서를 받을 예정이다.

코어플러드는 전세계적으로 230만대의 PC를 감염시켰으며, 그 중 백만대는 미국에 있는 것이다. 멀웨어를 제거하기 위해 처음에는 봇넷의 코어플러드 활동을 중단시키기 위해 감염된 컴퓨터에 메시지를 전송하여 봇넷의 C&C 서버를 다른 것으로 교체하였다. 하지만 컴퓨터가 다시 부팅하면 다시 활동이 가능하여 FBI는 완전히 멀웨어를 제거하는 방향으로 바꿨다.

FBI 조사관들이 코어플러드가 중동 대사관의 컴퓨터에 접근할 수 있는 마스터 키를 훔쳤다는 사실과 그 키를 러시아에 있는 서버로 전송했다는 사실을 발견했기 때문이다.

한국의 현대캐피탈 고객 67만명의 이름, 주소, 이메일 등 개인정보가 해킹당해 2011년 5월 19일 유출된 것으로 발표 되었다.

현대캐피탈 해킹 공격 사건에 해커 신모씨와 대출중개업체 팀장 윤모씨가 사용한 IP가 모두 9개 발견됐다.

사건 초기에는 신씨가 필리핀 등을 경유해 고객 42만명의 이름과 주소, 이메일 등을 해킹할 때 사용한 IP 두개가 검출됐다.

■ 지적저작권과 콘텐츠 해킹

하워드 스트링어 SONY 최고경영자(CEO)는 최근 집중적인 해킹 공격과 관련해 "우리가 해커의 표적이 된 까닭은 우리의 지적재산권과 게임 콘텐츠를 보호하려고 했기 때문이었다"고 밝혔다.

SONY는 2011년 4월 플레이스테이션 네트워크를 해킹 당해 7천700만명의 고객 개인정보를 유출 당한 것을 시작으로 세계 계열사에서 약 20여 차례 해킹을 당한 바 있다.

스트링어의 대답은 소니가 강력하게 게임 콘텐츠 등을 보호하려 하자 이에 반감을 가진 사람들이 소니를 집중 공격했다는 뜻이 된다.

스트링어는 "해킹을 당한 것은 소니만이 아니고, 지금 사이버 테러리즘이 세계적인 문제가 되고 있다"며 "이를 해결하기 위해서는 각국 정부가 뭔가를 해야 하는 아주 안좋은 상황"이라고 대답했다.

2011년 3월 10일 한국저작권위원회에 따르면 2010년 저작권을 침해한 스마트폰 앱이 웹하드와 P2P 사이트에서 적발돼 삭제된 건수는 총 1만1782건이었다. 전체 저작권 관련 적발 건수 8만5000건 중 13.8%이다.

2009년 11월 아이폰이 국내에 도입되기 전까진 저작권을 침해한 앱이란 게 없었지만, 1년 만에 스마트폰 앱이 저작권 침해의 주요 대상이 된 것이다.

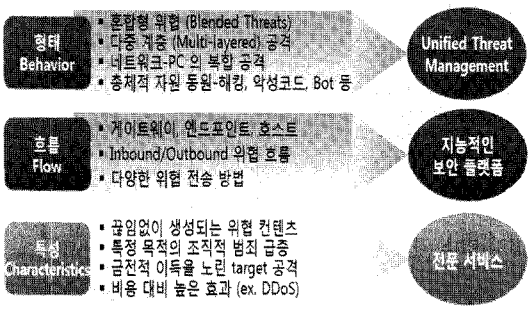
유료 앱을 해킹해 무료로 쓸 수 있게 퍼뜨린 사례가 대부분이었으며 타인의 DB나 저작권이 있는 콘텐츠를 무단으로 가져다가 앱으로 만든 사례도 많았다. 유료 앱을 해킹한 앱을 내려받는 것도 매우 간단하다. 일반적인 웹하드나 P2P 사이트에서 '아이폰', '안드로이드', '앱' 등으로 검색하면 해킹 앱 목록이 나타난다.

■ 방위산업체와 국방 부대 해킹

미국의 보안업체인 Trend Micro는 일본과 이스라엘, 인도, 미국의 방위산업체를 노린 표적형 공격을 확인했다고 2011년 9월 19일자 블로그를 통해서 발표했다. 피해기업 8곳을 확인되었다고 한다.

Trend Micro에 따르면, 지금까지 총 32대의 컴퓨터에 대한 불법침입이 확인되었으며, 공격에 사용된 네트워크는 2011년 7월부터 운용되어, 다른 표적을 노리며 계속 공격을 했다고 한다.

이번 공격에는 PDF를 첨부한 전자메일을 보내는 수법이 사용되었다. 1단계로 Adobe의 Flash와 Reade의 취약성을 노려 표적컴퓨터를 바이러스에 감염시키고, 공격용서버와의 접속을 성공시킨 뒤, 2단계에서 명령을 내려 해킹툴이나 멀웨어를 보내, 감염된 시스템을 제어할 수 있는 상태에 빠뜨렸다고 한다.



〔그림 12〕 해킹 공격 형태, 흐름, 특성

이러한 해킹 공격은 공격 목표에 따라 기술이 다양하게 사용되었으며 해킹 공격의 특징은 다음과 같다.

사이버보안 위협의 형태가 혼합된 복합 공격과 해킹 공격을 위한 다중 계층의 연동 공격이 증대하고 있어, Unified Threat management가 대두되고 있다.

해킹 공격 경로는 외부 해커로부터의 직접적인 공격, 내부 PC에 의한 outbound 위협이 있으며, 패킷, mail 등 다양한 도구를 활용하므로, 모든 패킷을 지능적으로 판단할 수 있어야 한다.

바이러스나 웜 등을 이용한 멀웨어 해킹은 특정 목적을 가지고 끊임없이 생성되며, 대부분 금전적 이득을 노린 목표 공격이므로, 전 분야의 위협에 대응할 수 있는 전문 서비스 체제가 필요하다.

4.2 해커(사람)의 동향 분석

해킹을 하는 해커와 해킹 공격을 수행하는 해킹 공격자가 있다. 해킹 공격자와 해커는 사람이 대부분이다. 해킹을 하는 해커는 어떻게 생산되고, 활동하게 되는가?

인터넷 포털사이트에 해킹의 기초부터 고급 단계까지 모든 게 널려 있었다. 2011년 4월 검색한 국내 포털사이트에서는 '좀비PC 만드는 법', '아이디 해킹하기', 등 해킹학원 강의 목록처럼 해킹 방법들에 관한 지식과 방법이 있다. 불법적인 해킹 기술 정보는 각종 블로그, 게시판 등 인터넷에 무분별하게 노출되어 있다.

또한 해킹을 직접 실행할 수 있는 해킹 툴(Hacking Tool)도 국내와 해외 온라인에서 쉽게 구할 수 있어 해킹에 대한 호기심과 자기만족감을 갖는 해킹 기술을 쉽게 배울 수 있다.

포털사이트 블로그의 '왕초보 해킹 배우기'에서는 해커가 되는 방법, 필수 유틸(Util), 해킹 사례는 물론 '주민번호 확인을 위한 코드', '카드번호 만드는 법' 등 해킹 기술이 상세히 묘사되어 있었다. 내용 중에는 해킹 적발 시 처벌되는 법령도 있었으며, '잘만 응용하면 모든 아이디, 비밀번호를 알아낼 수 있는 비법'이라는 내용으로 호기심을 부추겼다. 이론만이 아니라 실제 운영중인 온라인 게임사이트의 해킹 순서까지 예시돼 있었으며, 유명 해커들의 공공기관 해킹 성공사례는 영웅담처럼 미화되어 있었다.

해킹 프로그램인 해킹 툴도 쉽게 구할 수 있었다. 해킹 툴은 카사툴, 아포칼립스, 피시렛3.5, 고기툴, 넷봇 등 각종 사이트를 해킹하는 프로그램 등 다양했으며, 툴마다 사용방법이 자세히 묘사되어 있다. 일부 업그레이드된 해킹 툴은 온라인 카페 등에서 e메일 등을 통해 1만원 정도에 매매가 성행하고 있었다[5].

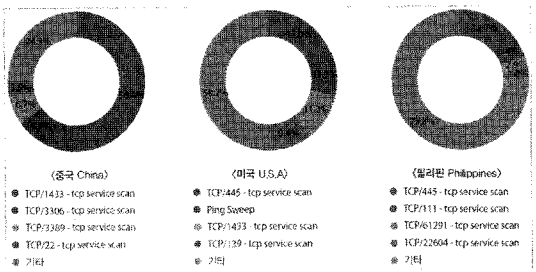
이와 같이 해킹은 PC를 사용하는 청소년들이 호기심으로 시작하지만, 해킹이 사회와 국가의 이슈로 등장하면서 인터넷을 통하여 해킹 관련기술을 습득하게 되고, 해킹 매니아로 성장하면서 해커학원이나 해커 동호인과 해커 클럽을 조직하여, 개인과 클럽을 통하여 해커로 활동하게 된다.

최근에는 해커에 대한 교육 정책적인 인력양성 필요성이 제기되면서, 정규대학에서 해커 관련 인력 양성이 되고 있고, 최근에는 정부에서 사이버국방학과를 지원하여 전문영역으로 졸업 후에 정보보호 조직에서 근무토록 할 예정이며, 민간에서는 각 학교 별로 해커 교육에 관한 관련 교육 내용이 개설되고 있다.

4.3 해킹 지역(국가)의 동향 분석

해킹 공격자를 토대로 하여 해킹 트래픽 유입이 많은 상위 3개 국가 별 공격 유형을 살펴보면 다음과 같다.

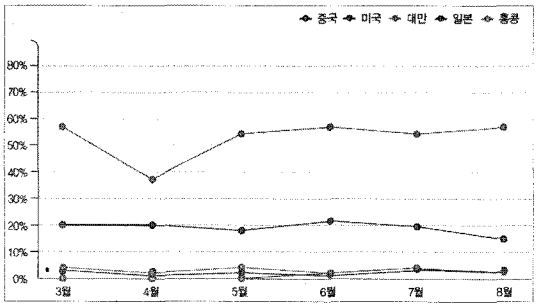
해외로부터 KISC 허니넷에 유입된 트래픽을 근원지



〔그림 13〕 허니넷 유입 트래픽 상위 3국가 별 공격유형

순위	2011년											
	3월		4월		5월		6월		7월		8월	
	국가명	비율	국가명	비율	국가명	비율	국가명	비율	국가명	비율	국가명	비율
1	중국	57.2%	중국	37.9%	중국	54.4%	중국	57.7%	중국	54.6%	중국	57.2%
2	미국	20.1%	미국	20.4%	미국	19.0%	미국	21.7%	미국	19.6%	미국	14.4%
3	대만	4.5%	대만	3.1%	대만	4.9%	일본	2.8%	대만	5.3%	필리핀	7.1%
4	일본	2.3%	브라질	2.6%	일본	1.9%	대만	2.7%	홍콩	4.6%	대만	3.5%
5	러시아	2.1%	일본	2.0%	인도	1.8%	홍콩	2.6%	싱가포르	2.1%	홍콩	3.1%
6	덴마크	1.8%	독일	1.0%	터키	1.6%	터키	1.3%	일본	2.0%	일본	2.1%
7	폴란드	1.6%	러시아	1.0%	독일	1.2%	인도	1.2%	러시아	1.7%	캐나다	1.9%
8	인도	1.6%	인도	0.9%	홍콩	0.9%	브라질	1.1%	브라질	1.6%	브라질	1.4%
9	영국	1.4%	터키	0.9%	러시아	0.8%	독일	0.9%	터키	1.6%	인도	1.1%
10	터키	1.3%	홍콩	0.9%	브라질	0.8%	캐나다	0.9%	필리핀	1.3%	러시아	1.0%
	기타	6.1%	기타	30.2%	기타	12.7%	기타	7.1%	기타	5.6%	기타	7.2%

〔그림 14〕 2011년 6개월간 허니넷에 유입된 유해 트래픽 국가별 비율



〔그림 15〕 허니넷에 유입된 국가별 유해 트래픽 추이

IP소재 국가별로 분석한 결과 중국으로부터 유입된 트래픽이 57.2%로 가장 많았으며 다음으로 미국(14.4%), 필리핀(7.1%) 순이었다. 중국으로부터의 트래픽은 TCP/1433, TCP/3306 포트에 대한 서비스 스캔이 가장 많은 비중을 차지한 것으로 나타났다[3].

V. 국가사이버보안정책 연구에서 해킹에 대한 소고

국가사이버보안정책을 위한 연구에서 해킹에 대한 고찰을 위해 전문가의 의견과 해킹 동향 분석을 토대로 하여 의견을 제시한다.

5.1 해킹 인력의 조직화

■ 중국 해킹 인력의 조직화

해킹 공격의 횟수와 트래픽의 근원지로 상위인 중국의 해커들의 동향을 분석해 본다.

중국에서는 공산국가이므로 국영과 민영의 구분이 애매해서 많은 해커들이 국가의 공동목표를 위해 일한다.

중국군은 1985년 국방과학기술정보센터를 설립해 정보전 연구에 들어갔으며 현재 컴퓨터 바이러스 부대, 반해커부대, 전자전 부대 등 3개의 사이버전 부대를 운영하고 있는 것으로 파악됐다.

컴퓨터 바이러스 부대는 1997년 중앙군사위원회산하에 설립됐으며 100여명의 요원이 활동하고 있다. 2000년 8월에 중국과학원 산하에 설치된 반해커부대는 외국의 해킹을 차단하고 있다. 2003년 설치된 전자전부대는 7개 군구 가운데 베이징, 광저우군구 등 4대군구에 설치돼 있으며 미국 명문 매사추세츠공대(MIT) 유학생 등 약 2천명이 배치돼 해킹 기술 개발 연구을 하고 있다. 이들은 정보전 수행을 위한 컴퓨터시뮬레이션 개발, 모의 전술훈련지원과 함께 외국정부기관의 자료를 빼내는 임무를 수행하고 있다. 이들 외에 홍커(Red Hacker)로 불리는 약 100여명의 해커들이 수시로 미·일·대만 등에 대해 집중공격을 하고 있는 것으로 분석됐다[6].

2010년 7월 '인터넷 기초총부'라는 사이버전 부대를 창설하여 운영하고 있는데, 이 부대의 해킹 기술력은 세계 최고 수준인 것으로 평가받고 있다.

중국의 민영 해커는 1990년대 흑객(黑客, Dark Visitor)로 칭하며 해커 활동은 조직화되어 중국 정부와 연관된 첩보 조직으로 탈바꿈했다. 해커들은 애국심으로 무장되었고, 중국 인민해방군(PLA)에 의해 디지털 첩보 및 데이터 탈취 세력으로 조직화 되고 있다.

중국에서 해커들이 조직화된 것은 1997년 "그린아미(Green Army)"가 처음이다. 1998년 인도네시아에서 반중국 소동이 벌어진 직후에는 "레드 해커 얼라이언스"가 구성됐다. 이후에 많은 해커 조직이 결성됐다가 해산됐다가 재결성되곤 했다.

등소평이 시장경제를 도입하면서 2000년대 해커들은 해킹 실력을 이용해 돈을 벌 수 있다는 생각을 하게 되

〔그림 16〕 "미국 제국주의 박살내자" 흑객 싸이트 문구

었다. 많은 해커들이 보안 컨설턴트로 일하기 시작했다. 스콧 헨더슨이 쓴 "흑객(Dark Visitor)-부제는 '중국 해커 세계의 내막" 책[7]에 이런 내용이 요약되어 있다.

2005년부터 중국 해커들은 두 가지 생각을 하기 시작했다. 정치적 모티브인 애국심과 경제적 모티브인 돈이 그것이다. 중국이 정치적 입지와 경제적 입지를 다져야 한다는 필요성에서 홍커 유니온이나 그린아미와 같은 해커 그룹을 조직화하는 계기가 되었다.

인민해방군이 해커들을 기업화하고 청두기술대학 등 대학에서 프로그램(해킹 기법)을 가르치기 시작하면서 국가를 위해 일하는 '국가일꾼(State Actor)'이란 소명의식으로 더욱 보편화됐다. 이들은 모두 국가일꾼으로 일하고 있다고 생각한다[8].

■ 북한 해킹 인력의 조직화

북한은 지도자 김정일위원장의 직접 지시로 정예의 해킹부대를 운영해 남한의 국가기관과 연구기관을 대상으로 정보를 수집한다"고 하였다. 김정일은 2007년 3월 평양시 근교의 한 공장을 시찰하면서 "현대전은 전자전이다. 적의 전자전 능력을 마비시킬 수 있는 전술을 개발하라"고 지시하였다[2].

북한의 최고 권력기관인 노동당 비서국 산하에 35호실을 설치, 인터넷을 통해 정보 수집과 정보 분석 등에 열중이다. 지난해엔 정찰총국 산하 사이버부대를 121국으로 승격시킨 뒤 병력을 기존의 6배인 3천명으로 늘렸다. 미 폭스뉴스는 북한의 사이버 전쟁 수행 병력이 3만명이라며 CIA의 사이버전 능력과 맞먹는다고 보도했다[9].

북한군에서 해커를 조직적으로 양성하는 핵심기관은 평양시 미림동에 위치한 일명 '미림대학'으로 알려졌다. 정식 명칭은 지휘자동화대학이었는데, 김일군사대학으로 개명했다고 한다. 1986년 옛 소련 국방부의 지원으로 세운 5년제 대학인 미림대는 매년 100여 명의 컴퓨터 전문가를 키워왔다고 전해진다. 군 관계자는 "미림대 출신을 주축으로 다른 대학 '컴퓨터과학' 전공자를 합쳐 정예 150여 명을 추린다. 이들이 기본교육 1년을 마치면 군관(장교)으로 임관된다"고 말했다.

이후 정찰총국이 직할 운영하는 압록강군사대학(평양시 사동구역 소재, 대남공작원 양성기관으로 알려짐)으로 보내 '사이버전사'로 양성한다. 이들 중 우수자를 선발해 신분을 세탁한 뒤, 중국·러시아·유럽 등에 소재한 박사급 과정에 유학도 보낸다. 복귀 후에는 정찰총국 산하 '110호연구소'와 총참모부 산하 '전자전지도국'에 배치된다."

110호연구소와 달리 전자전지도국은 지금껏 언론에 한 번도 노출된 적이 없는 북한군 기관이다. 우리 군은 전자전지도국이 7개 대대로 구성됐으며, 야전전자전을 지원·수행하는 부대로 파악하고 있다.

110호연구소와 전자전지도국의 임무는 확연히 달라 보인다. 군 관계자는 "상급기관의 성격을 반영한다"고 말했다. 익히 알려졌듯 정찰총국은 대남공작 등 특수전을 담당한다. 반면 사실상 국방위 직속으로 추정되는 총참모부는 반역과 테러를 방지한다. 명칭상으로는 우리의 합동참모본부와 유사하지만 기능은 다른 셈이다. 이런 성향을 반영해 110호연구소는 공격 성향의 부대, 전자전지도국은 방어 성향의 부대로 전해졌다.

전자전지도국은 평시에는 컴퓨터시스템 보안에 치중하지만, 전시에는 야전군과 상대를 향해 전자전을 수행한다.

110호연구소는 약 1천명 규모의 해커를 보유했다고 추산된다. 금융·공항·항만·위성항법장치(GPS) 등에 혼란을 야기시킨다는 임무가 주어진 듯하다. 전시에는 국방지휘체계가 목표다. 정부와 주한 미 8군이나 연합사령부는 물론이고 펜타곤·중앙정보국(CIA)·태평양사령부 등을 공격한다." "만약 이번 농협 해킹이 북한의 소행이라면 사건 성격상 110호연구소가 주도했을 확률이 높다"면서 "중국 선양(瀋陽)에 마련된 이들의 사이버거점이 공격의 진원지일 것"이라고 추정했다[2].

미국군은 2010년 초에 발표한 국방검토보고서(QDR)에서 육·해·공·우주 외에 사이버 공간을 '제5의 전쟁터'로 추가하고 5만 명 규모의 사이버 사령부(USCYBERCOM)를 공식 설립했다. 공군 산하에 사이버 전쟁 인력 3만 명을, 육군 산하에는 2만1천명을 편성했다. 우주사령부는 매년 사이버 작전장교 4백명을 양성할 계획이다.

사이버 사령부의 정확한 병력 규모는 공개되지 않았지만 250개의 사이버 부대에 약 5만여 명의 장병이 복무 중인 것으로 해외에서는 추정한다[10].

미국은 민간 해커 가운데 무려 25%를 연방수사국(FBI)의 비밀정보원으로 활용하고 있다고 영국 일간 가디언이 최근 보도했다[9].

5.2 해킹 기술의 집적화

해킹 기술이 급속하게 진화하고 있다. 최근에 국가간

의 물리적 분쟁이 사이버월드에서 출발한 사이버국방으로 인식의 전환이 확산되면서, 해킹 기술의 집적화는 미사일이나 핵폭탄과 보다 더 정밀해지고 있다.

블랙햇 보안 컨퍼런스에서 보안 전문가들은 모바일과 와이파이나 블루투스 신호에서 정보를 탈취하는 무선 해킹을 시연했다. 일명 '워 플라잉'이라 불리는 진화된 해킹 수법이다. 얼마 전까지 자동차를 이용해 실외 무선신호로부터 정보를 훔치는 '워 드라이빙'이 성행했고, 이제는 무인항공기를 이용한 해킹이 가능해졌다는 것이다. 워 플라잉은 더 광범위한 무선 네트워크로부터 정보를 수집할 수 있어 더욱 치명적이다. 해커들은 스니핑 프로그램을 이용해 무선망을 사용하는 개인들의 정보를 탈취해 나가는 수법을 활용하고 있다.

컨퍼런스에서 워 플라잉을 해킹을 시연한 보안 엔지니어 리치 퍼킨스는 "(시연 대상자가)휴대폰을 사용하면 집에서 회사까지 보안이 영향을 미치지 않는 네트워크 영역에서 해킹 가능성이 있음을 확인했다"면서 "개인과 정부 및 주요 기관들도 모두 무선 보안에 무방비 상태이기 때문에 대책마련이 시급하다"고 지적했다[11].

해킹 기술의 집적화는 해킹의 내용과 활동을 변화시키고 있다. 중국의 흑객인 해커들의 초기 활동으로는 웹페이지에 침투하여 위변조 정도이었으나, 황신이 최초의 중국제 트로이안 목마인 '글래시어' 멀웨어를 제막한 후 트로이안 활용이 급증했다.

중국의 해커들의 실력이 쌓임에 따라 피공격자가 공격자의 의도대로 변종을 발생시켜 최종 목표를 해킹 공격하는 형태의 해킹 기술의 집적화를 가져왔다.

중국 해커들은 중간에 좀비PC나 중간 숙주들이 알수 없도록 악성 코드와 멀웨어 다운 사이트가 링크된 이메일을 보낼 수 있게 되었다[12]. 이런 수법이 피싱과 파밍으로 연결되어 금전적인 수익을 창출하고, 수익 분배와 집적된 해킹 기술로 더욱 사회공학적인 해킹 기술을 집적한 것으로 발달하고 있다.

이러한 해킹 집적 기술은 해킹 인력의 조직화와 더불어 자금과 인력을 확보한 상태에서 해킹 전력과의 시너지효과를 만들면서 급속하게 진화하고 있다.

5.3 해킹 조직의 집중화

위 자료에서 살펴보면 중국, 북한, 미국은 해킹 조직에 대한 컨트롤 타워를 구성하여 각 군부대와 민영조직을 집중화하여 국가사이버보안과 공격전력에 대한 역량을 배가 시키고 있다.

또한 자생적으로 발생한 민영 매니아 조직들도 해킹 조직을 집중화하는 경향으로 나타나고 있다. 최근 정치적, 이념적 방향에 목적을 둔 해킹 활동을 핵티비즘(Hacktivism)이라하는데, 해킹(Hacking)과 정치적 목적을 위한 행동을 뜻하는 액티비즘(Activism)이 합쳐진 단어의 뜻이다.

위키리크스(www.wikileaks.org) 폭로 사이트를 만든 줄리안 어산지가 기소되는 것을 계기로 위키리크스를 지지하는 세력들에 의한 핵티비즘 활동이 증가하고 있다. 위키리크스의 후원 계좌를 폐쇄한 페이팔 등에 사이버 공격을 가하는 한편, 위키리크스의 내용들을 복제한 미러(Mirror) 사이트들을 만들어 퍼뜨리고 있고, 위키리크스를 지지하는 비공식 해킹 세력인 Anonymous는 위키리크스를 탄압하는 세력들에 대해 전쟁을 선포하고 해당 기업들에 대한 사이버 공격을 계속할 것이라고 밝혔다.

또한 이탈리아 총리 시리오 베를루스코니 언론 자유 억압에 대한 항의 표시로 이탈리아 정부 홈페이지를 공격했다.

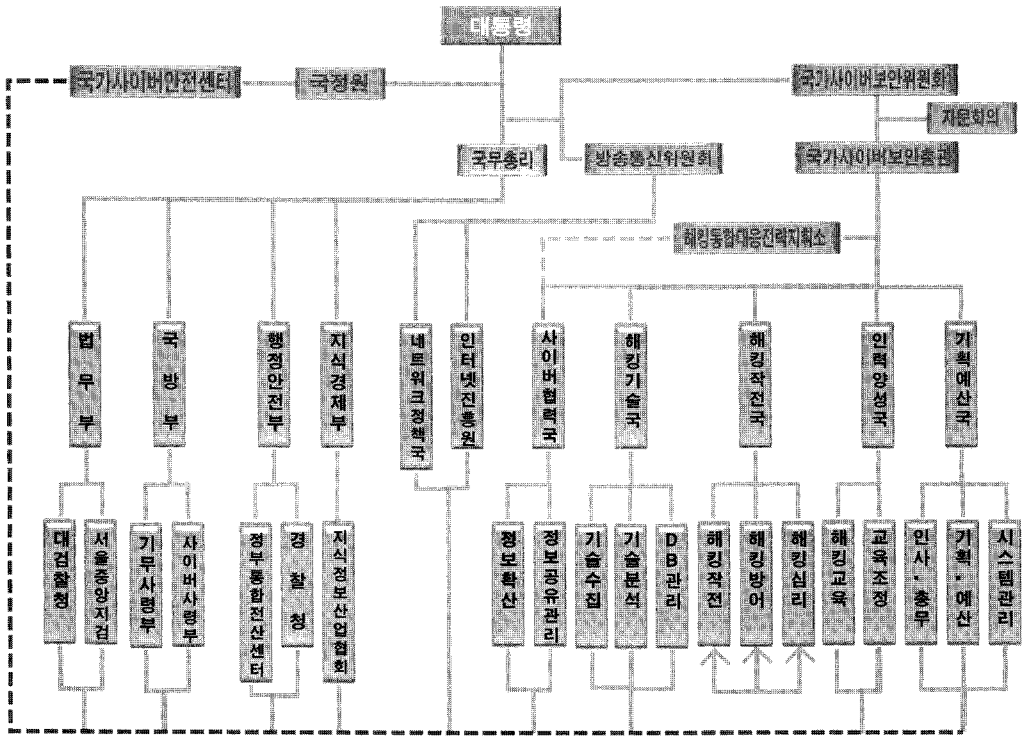
또한 201년 구글의 중국 대륙 철수 결정을 만들었던 구글 사이트 해킹 사건배후에는 중국 공산당의 공격 지시가 있었던 것으로 드러났다. 주베이징 미국 대사관에서 작성한 외교 문서에 다르면 "중국 공산당 고위 관계자가 구글 사이트를 통해 자신을 비판하는 글을 확인한 후 구글에 악감정을 가지고 해킹 공격을 지시했다"는 내용이 담겨 있었다.

이와 같이 해킹에 대한 군사적, 정치적, 경제적 목적과 해커 개인과 해커 조직의 목적이 일치하거나, 동조화되면서 해킹 조직의 집중화 현상이 나타나고 있다.

5.4 국가사이버보안정책에서 해킹 전략 소고

개인 해커들의 해킹 공격들의 목적은 인터넷 서비스 업체들의 DB 서버를 공격하여 가입자들에 대한 개인정보를 탈취하여 불법적으로 금전거래를 하거나, 온라인 게임 계정을 탈취하여 게임 아이템 탈취, 게임 사이트에 대한 DDoS 공격 협박으로 돈을 받아 챙기는 개인 경제적인 목적의 해킹 공격이 성행 하였다.

2009년 7.7 DDoS공격과 2011년 3.4DDoS공격, 2011년 4월 발생한 NH 금융전산망 마비 사태와 3,500만명의 NATE 메일 사용자와 2,500만명의 싸이월드 사용자의 정보가 해킹당하면서, 이제는 해킹이 국가사이버보안정책에서 다루어져야 할 필요성이 있다.



〔그림 17〕 국가사이버보안법에 의한 조직 구성(제안)

특히 국가의 인프라인 네트워크와 중요 제어 시스템을 무력화시킬 수 있는 '스턱스넷'과 같은 사이버 무기가 개발되면서 사이버전은 내부적으로는 국가보안의 문제로, 외부적으로는 외교적 갈등으로 확대되고 있다.

하지만 해킹 공격으로 인한 국가적인 피해에도 불구하고 범인 색출이나 책임소재 재판이나, 국가적인 보복이 어려운 사이버전의 특성을 깨우치게 된 각국은 경쟁적으로 사이버 전력 증강에 나서고 있다.

따라서 저자는 개인적인 의견으로 국가사이버보안정책에서 해킹 전략을 다음과 같이 제안한다.

■ '국가사이버보안법' 제정

국가사이버보안법을 제정하여 국가사이버보안에 대한 추진전략을 세우고 제도적으로 시행되게 해야 한다. 대통령직속으로 상설기관인 '국가사이버보안위원회'를 두고 '국가사이버보안총관'을 대통령이 직접 임명한다.

■ '국가사이버보안법 시행령' 제정

'국가사이버보안위원회'의 조직은 국가사이버보안법에 의하여 [그림 17]처럼 구성을 제안한다.

같은 장소에서 같은 시각에 정보를 공유하고 해당 각 부처에 협력과 연락을 담당하는 사이버협력국, 해킹 기술을 수집하고, 해킹 기술을 분석하며, 해킹 기술의 DB를 관리한다.

해킹작전국은 해킹 작전과 해킹방어, 해킹심리를 내용으로 한다. '인력양성국은 해킹교육 내용을 정리하여 해킹 전문가로 하여금 교육을 하게하고, 다른 기관의 해킹 전문가가 교육기관의 교육을 담당하여 정보공유와 기술 확산을 위한 교육 조정을 한다.

기획예산국에서는 국가사이버보안총관의 보좌를 하며 인사와총무, 그리고 기획과 예산을 담당하고, 해킹툴 수집, 개발에 필요한 해킹 기술 DB서버 등 서버의 접근제어와 보안등급 등을 관제 관리한다.

기존, 사이버공격대응체계의 대응시간 지연문제를 극복하고, 긴급한 국가위기에 대한 대응 역량을 강화하기 위하여, 해킹통합대응전략지휘소는 민·관·군 영역별 사건을, 통합대응해서 실시간으로 지휘한다. 또한, 정보공유(같은 DB사용) 같은 장소에서 협력관들은 시행령으로는 협력관에 대한 협조결재 제도가 반드시 시행되어야 한다.

■ '국가사이버보안위원회' 조직 구성

대통령을 위원장으로 하는 국가사이버보안위원회에서는 '국가사이버보안총관'을 부위원장으로 하여 국가사이버보안에 관한 컨트롤타워를 구축한다.

자문회의와 사이버협력회의를 두고, 해킹기술국, 해킹작전국, 기획국, 인력육성국, 기획예산국을 만들어야 한다.

국가정보원의 국가사이버안전센터와 정보및보안기획조정관이 협력관으로 참여한다. 국방부의 기무사령부, 사이버사령부에서 참모장급이 협력관으로 참여한다. 법무부에서는 대검찰청과 서울중앙지검이 협력관으로 참여한다. 행정안전부에서는 정부통합전산센터와 경찰청 사이버테러대응센터가 참여한다. 방송통신위원회 KISA와 지식경제부 지식정보산업협회가 산업기술부분에 참석한다.

■ 국가사이버보안 자문회의

'국가사이버보안총관'은 조직의 변화, 국가위기대응, 해킹 기술의 동향 분석, 해킹 인력양성, 등에 대하여 해킹 자문교수나, 전문가를 구성하여 자문회의를 수행하고, 정책과 전략에 반영한다. 건의된 사항은 대통령에게 보고하여 처리 할 수 있다.

■ 국가사이버보안 협력회의

'국가사이버보안총관'은 정기와 수시로 국정원, 방송통신위원회, 법무부, 국방부, 행정안전부, 지식경제부 등의 국가사이버보안전략 회의를 소집하고 대통령에게 보고한다.

사이버협력회의는 사이버협력국을 통해 파견된 부처와 수시로 협의하여 국가사이보안상태와 해킹동향을 보고하여 정보를 공유하고, 공동 대응하여야 한다.

■ 해킹 프로세스 전략

국가사이버보안정책에서 해킹 목표에 따라서 각 단계인 1) 준비기, 2) 시작기, 3) 활동기, 4) 확산기, 5) 정리기로 나누어져 평가 목표를 정량적으로 설정 한 후에 시행되어야 하며, 해킹 프로세스 전략은 해킹 결과에 따라서 각 단계인 1) 탐색기, 2) 준비기, 3) 잠복기, 4) 해킹 실행, 5) 역추적 삭제 등의 프로세스를 기본으로 하여 각 프로세스의 인력과 예산과 산출물, 결과 피드백을 시행한다. 현재 국가정보원의 국가사이버안전센터 및 한국인터넷진흥원의 인터넷침해대응센터에서 사이버위협 대응 단계에 적용하는 정상, 관심, 주의, 경계, 심각 단계로 분류하고 있다.

목표는 본 연구에서 제안하는 내용으로 분류해 본다면 해킹 인력의 조직화, 해킹 기술의 집적화, 해킹 조직의 집중화 등으로 분류해 볼 수 있다.

■ 해킹 전략 추진 방법론

해킹과 방어는 창과 방패의 싸움이라고 한다. 앉아서 기다리는 방패전략은 방어가 아니다. 창과 방패의 싸움에서 창을 연구하고 집중해야 방패의 역할과 기능을 충실히 수행 할 수 있다.

현재 공공기관의 전략은 방패의 전략에서 창과 방패의 전략으로 수정해야 하면서, 특히 활동기, 확산기, 정리기로 갈수록 창으로도 방패의 역할을 수행하면 효과가 있다.

다음은 '국가사이버보안위원회'의 조직에 대하여 저자의 의견을 제안한다.

▲ 사이버협력국

사이버협력국은 정보공유팀과 정보확산팀을 둔다. 국가정보원의 국가사이버안전센터와 정보보안기획조정관 등이 협력관으로 참여한다. 국방부의 기무사령부, 사이버사령부에서 참모장급이 협력관으로 참여한다. 법무부에서는 대검찰청과 서울중앙지검이 협력관이 참여한다. 행정안전부에서는 정부통합전산센터와 경찰청 사이버테러대응센터가 참여한다. 방송통신위원회 KISA가 지식정보산업협회가 참석한다. 지식경제부 사이버안전센터가 참석한다.

사이버협력국에서는 반드시 같은 장소, 같은 시간에 해킹과 대응 전략지휘소와 같은 정보공유(같은 DB사용)를 위해 근무하며, 협력관들은 사이버협력회의에 각 부처 의원들을 보좌하여 참여할 수 있다.

따라서 업무 시행을 위해서는 즉시로 같은 공동의 작전에서 협력관에 대한 '협조결재 제도'가 반드시 시행되어야 한다.

▲ 해킹 작전국

해킹과 방어는 창과 방패의 싸움이다. 앉아서 창의 공격을 기다리는 방패는 항상 늦는다. 지금까지의 공공의 전략에 대한 패러다임의 변화를 가져와 실시간 업데이트 하는 적극적인 변화가 필요하다. 해킹 작전은 '국가사이버보안'과 '국가사이버패권'이라 양주머니에 손

을 넣고 상대 국가, 상대 조직, 상대 해커에 따라서 공격과 우회공격이라는 양면의 동전을 선택해서 국가사이버전력으로서 사용되어야 한다는 점이다.

준비기에는 방패를 통하여 Cooperative Defense 전략을 구축하여야 한다. 해킹 방어는 기존의 국가정보원이 주축이 된 CERT/CC를 활용하고, 행정안전부의 정부통합전산센터와 정보보안산업계가 상설기관을 만들어서 협력하여야 한다. 또한 법과 제도를 만들어서 예산과 인력을 확보하고 국가사이버보안정책을 준비하여야 한다.

시작기와 활동기에서는 창과 방패의 양손 전략으로 Strategic Response를 하여야 한다. 해킹 공격 전략을 추진하고, 프로세스를 정형화, 정량화해야 하지만 해킹 기술의 변화를 주목하여 창의 입장에서 방어를 구성하여야 한다.

확산기와 정리기에는 Progressive Response를 사용하여야 한다. 사실 창으로도 방패의 역할을 할 수 있다. 이때에는 창과 방패의 역할만 있을 뿐, 사이버공간에서는 창과 방패의 구분이 없다.

정리기에는 Active Attack이 주요한 정책이다. 기존의 투입된 인력과 장비를 활용하면서 국가전체적인 하나의 시너지를 이룬다면 창과 방패가 하나이므로 굳이 구분 할 필요가 없다.

해킹의 주체는 사람인 해커이다. 따라서 해커의 심리전에 관한 대응이 필요하다.

해킹에서는 아군과 전국의 식별이 어렵고, 해킹을 수행하고 방어하는 인간의 내면을 파악하기는 더욱 어렵다. 그렇다고 지금처럼 폐쇄적인 조직의 커튼 뒤의 전략으로는 0.1초에 승부가 나는 치열한 사이버전쟁에서 절대로 이길 수 없다.

최근에는 정치, 경제, 사회, 문화에 걸쳐 SNS, Twitter, 홈페이지, SMS, MMS, 콘텐츠, e-mail 등이 사회공학적인 방법으로 적극적으로 사용되므로, 이들을 통한 해킹기술, 해킹 툴, 해커에 관한 동향정보를 적절히 활용하고 이를 수단과 국가사이버보안을 위한 목적으로 사용할 수 있어야 한다.

▲ 인력 양성국

해킹의 주체는 해커와 해킹 기술 그리고 해킹 툴이다. 그중에서도 중요한 요소는 해커이다. 지금까지의 자료를 분석해 보면 해킹의 기술이 집적되지 않고, 조직이 집중화되기 전까지의 해커는 해킹 매니아 출신이 해커의 인력의 중심에 있다.

이들은 중학생때부터 호기심으로 출발하여, 고등학교 과정에서 일반대학진학 교육과정보다 해킹에 대한 시간과 노력을 집중하여, 상위권 대학 진학보다는 해킹 관련 학원이나, 전문대학과 일반 대학교 등에 진학한다. 따라서 이때의 중요한 요소는 해커의 관심과 적성이 주요소이다. 따라서 이들의 적성과 진로를 가이드하고 흥미를 유발하여, 해커로서도 사회적인 관심과 국민으로서 활용가능성에 맞는 전략을 취하여야 한다.

이들이 대학을 진학하면 상급학년에 국가사이버보안 전략적 요소에 관한 접목으로 그들이 국가가 필요로 한다고 하는 사명감을 주고, 실전에 투입할 수 있는 전략과 전술을 지도하는 대학원 진학을 통하여 국가사이버보안전략에 대한 교육과정을 이수하게 된다.

포인트는 중학교 졸업전 고등학생 해킹인력의 조직화, 고등학교 졸업 전 대학교 해킹인력의 조직화, 대학교 졸업전 대학원 해킹인력의 조직화가 필요하면 조직화도 해킹그룹과 쉽게 친 할 수 있는 선생님이나 교수가 중심이 되고 관계기관이 협조와 자문 및 지원을 하여야 한다는 것이다.

▲ 해킹 기술국

해킹의 기술은 기술수집팀을 통해 해킹 기술 DB서버에 수집되어야 한다. 우선 국내에서 전문가가 사용하는 기술이 정의되어 기술DB서버에 집적되어야 한다. 중국과 미국의 해킹 기술은 세계적 수준이다. 중국과 미국뿐만 아니라 북한과 소련의 해킹 기술을 수집하여야 한다.

해킹 기술 DB서버에 해킹 기술을 집적하고 분석하며, DB사용에 관한 접근통제 및 보안관리는 기획예산국에서 관리하여 입력, 출력을 따로 관리 한다.

해킹의 변천사를 분석해 보면 트렌드가 있다. 따라서 해킹의 트렌드와 기술을 정확하게 예측하고, 대응해야 한다. 해킹은 인력+기술+자금+인프라 등의 변수가 결정하므로 기술 수준이 상위에 오르면 해킹 공격 시나리오와 해킹 대응 시나리오는 시간의 차이만 날 뿐이다.

▲ 해킹 조직의 집중화

중국, 북한, 미국은 해킹 조직에 대한 컨트롤 타워를 구성하여 각 군부대와 민영조직을 집중화하여 국가사이버보안과 공격전력에 대한 역량을 배가 시키고 있다.

또한 자생적으로 발생한 민영 매니아 조직들도 해킹

조직을 집중화하는 경향으로 나타나고 있다.

해킹 조직의 집중화 현상은 인터넷을 통한 사이버국경이 모호해지고, 국가간의 이념적, 정치적, 경제적인 갈등 구조와 맞물리면서 더욱 심화 되고 있다. 그 결과 개인간의 그룹활동의 범위를 넘어서, 가상공간인 사이버상에서 그룹화되고, 국가지원하에 조직화, 그룹화되면서, 개인이 해킹 조직을 관리하기에는 어려운 실정이 되었다.

따라서 해킹 조직의 집중화의 동향을 파악하고 분석해서 국가와 국민을 위한 해커 개인에 대한 국민으로서 애국심 및 당위성을 부여하여 해킹 조직의 발전이 국가와 국민의 보안에 기여하는 당위성에 관한 관심과 노력이 필요한 시점이다.

VI. 결 론

기존에 국가간의 갈등을 해결하는 전쟁의 수단에서 미사일, 포탄 등 물리력을 동반한 인적, 물리적 전쟁은 전쟁비용과 인명살상이 직접적으로 이루어져, 국민의 지지와 세계 여론의 호감을 받는 것이 점점 더 어려워지고 있는 것이 사실이다.

지금까지 핵보유와 전쟁의 전력을 통해 '국가간패권'을 장악했던 국가들에 대해 해킹이나 친구의 이메일 로 위장한 트로이목마나 봇넷 같은 악성코드 등의 기법을 활용하면서 DDoS 공격으로 순식간에 국가의 중요 네트워크와 작전 수행 능력을 무력화할 수 있다.

이제 세계는 '국가사이버보안'과 '국가사이버패권'이라 양주머니에 손을 넣고 상대국가에 따라서 보안과 공격이라는 양면의 동전을 꺼내서 사용하고 있다. 즉 해킹이 국가사이버보안의 중요 전력파워로서 사용되고 있다는 점이다.

초고속 인터넷을 통하여 세계는 더 이상 국경의 구분이 없고, 언제든 신속하게 공격이 가능하고, 아군 적군의 물리적인 구별이 불분명하고, 공격 지점과 방어지점이 구별되지 않는 비대칭 전력으로서 해킹 대국이라고 하는 중국과 미국 등 세계의 경쟁속에 한국(남한)은 북한과 적대적 관계에 있다.

따라서 본 연구에서 해킹 인력의 조직화, 해킹 기술의 집적화, 해킹 조직의 집중화는 국가사이버보안정책의 해킹에 대한 필수적인 핵심 요소로서 판단된다.

이를 실현하기 위한 개인적인 저자의 의견을 제안하였다. 본 논문에서는 국가사이버보안을 위한 '국가사이버보안법' 제정과 '국가사이버보안법 시행령' 제정, 국가사이버보안 자문회의, 국가사이버보안 협력회의, 해킹 프로세스 전략, 해킹 전략 추진 방법론, 사이버협력국, 해킹 작전국, 인력 양성국, 해킹 기술국에 관한 의견을 제안하였다.

참고문헌

[1] 김광현, "해킹에서 사이버 첩보활동으로…중국 해커의 변화", 한국경제, 2011.06.13.

[2] 김상진, "후계체제 속 'IT 지도자' 치적에도 도움 - 110호연구소·전자전지도국에 '사이버 전사' 집결돼", 월간중앙, 2011.08.05

[3] KrCERT/CC, 2011년 08월 인터넷침해사고 동향 및 분석 월보

[4] 전성철, 장관석, ["농협 해킹은 北 소행"]검찰 "농협 해킹, 北 정찰총국이 7개월간 준비", 동아닷컴, 2011.05.04.

[5] 이용권, "'좀비PC 만드는 법'? 대한민국은 '해킹천국'", 이타임즈, 2011.04.12.

[6] 최현수기자, 중국 해커부대 전세계 공격, http://news.kukinews.com/article/view.asp?page=1&gCode=pol&arcid=0921287339&cp=nv, 2009.05.13.

[7] Scott Henderson, "Dark Visitor", Jun 7, 2011.

[8] 광파리의 글로벌 IT 이야기, "해킹에서 사이버 첩보활동으로…중국 해커의 변화", 2011.06.13.

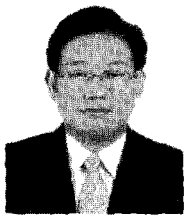
[9] 배성재기자, 제5의 전장 '사이버 대전'격화, http://news.hankooki.com/lpage/world/201106/h2011061902302122450.htm, 한국일보 국제면, 2011.06.19.

[10] 최상연외 7명 기자, 지구촌 중국, http://article.joinsmsn.com/news/article/article.asp?total_id=4556428&ctg=13, 중앙일보, 2010.10.22.

[11] 김희연, "진화하는 해킹 기술…"사회 시스템까지 위협"", 지디넷, 2011.08.14.

[12] 변정수 책임연구원, "사이버 테러리즘과 해킹", 코센21 칼럼 12th, 2011.09.17.

〈著者紹介〉



박 대 우 (Dea-Woo Park)
종신회원
1998년 8월 : 숭실대학교 컴퓨터학과 (공학석사)
2004년 2월 : 숭실대학교 컴퓨터학과 (공학박사)
2004년 3월 : 숭실대학교 겸임교수
2006년 8월 : 정보보호진흥원(KISA) 선임연구원
2007년 3월 ~ 현재 : 호서대학교 벤처전문대학원 교수
<관심분야> Hacking, CERT/CC, 침해사고대응, e-Discovery, Forensic, 사이버국방, 정보보호, 유비쿼터스 네트워크 보안, WiBro 보안, VoIP 보안, 스마트폰 및 이동단말 보안