FOCUS 3

국내 주요 인터넷 사고 경험을 통해 본 침해사고 현황

신종환

지난 10여 년간 우리나라의 정보통신기술의 발달, 특히, 정보화와 인터넷 관련 기술의 발달은 업무 생산성과 효율성의 향상과 언제 어디서나 필요한 정보를 쉽게 취득, 가공, 재생산해서 지식정보화사회를 가져왔다는 점에서 우리사회의 발전에 공여하는 바가 크나 그와 더불어 모든 사회가 인터넷으로 상호 연결되어 인터넷 상에서 침해사고가 발생 시 그 피해는 기하급수적으로 늘어나며, 그 파장은 모든 영역에 미친다는 점에서 정보사회의 발달은 양날의 칼이라 하지 않을 수 없다. 따라서, 이러한 정보통신기술의 순기능을 최대한 활용하고 역기능을 최소화하기 위해서는 사회 모든 영역과 구성원들이 인터넷 침해사고에 대한 관심과 방지를 위한 노력에 신경을 기울여야 한다. 지난 10여 년간의 주요 인터넷 사고 경험을 되돌아봄으로써 정보통신기술의 안전한 사용을 통한 신뢰할 수 있는 사회 구축을 위해 나아가야 할 방향에 대해 알아보고자 한다.

Ⅰ. **서론**

Ⅱ. **최근 10여 년간 발생한 주요 인터넷 침해사고**
1. 1.25 인터넷 침해사고('03년)
2. 리니지게임 명의도용 사고('06년)
3. 옥션 해킹사고('08년)
4. 7.7 DDoS 사건('09년)
5. 3.4 디도스 대란('11년)
6. SK컴즈 개인정보 유출사고('11년)
7. 3.20 및 6.25 사이버 공격('13년)

Ⅲ. **시사점**

한국인터넷진흥원 조사분석팀 책임연구원(johwani@kisa.or.kr)

Ⅰ. 서론

지난 10여 년간 우리나라의 정보통신기술의 발달, 특히, 정보화와 인터넷 관련 기술의 발달은 업무 생산성과 효율성의 향상과 언제 어디서나 필요한 정보를 쉽게 취득, 가공, 재생산해서 지식정보화사회를 가져왔다는 점에서 우리사회의 발전에 공여하는 바가 크다 하겠다. 또한 이는 전 세계적인 현상으로 우리와 같이 자원이나 영토가 부족한 국가에서는 지식창조 산업인 정보통신기술을 적극 활용하여 선진국으로 도약하여 여러 강대국들과 경쟁할 수 있는 중요한 근간으로써 올바른 방향으로 나아가고 있는 것이라 하겠다.

그와 더불어 이러한 정보화 사회의 순기능에도 불구하고 모든 사회가 인터넷으로 상호 연결되어 네트워크화되고 국가기관 및 민간기업의 대부분의 활동이 인터넷 기반으로 이루어지고, 심지어는 개인의 활동 역시 인터넷 기반으로 이루어짐에 따라, 단순한 인터넷 침해사고의 경우에도 상황에 따라서는 그 피해가 심각하게 나타나는 인터넷 네트워크 사회에 우리는 살고 있다. 그에 따라, 인터넷 상에서 침해사고가 발생 시 그 피해는 순식간에 기하급수적으로 늘어날 수 있으며, 그 파장은 모든 영역에 미친다는 점에서 정보사회의 발달은 양날의 칼이라 하지 않을 수 없다. 이러한 정보통신기술의 순기능을 최대한 활용하고 역기능을 최소화하기 위해서는 사회 모든 영역과 구성원들이 인터넷 침해사고에 대한 관심과 방지를 위한 노력에 신경을 기울여야 한다.

하지만 현실은 그렇지 않은 것 같다. 최근 10여 년간 다양한 인터넷 침해사고가 발생하고 있지만 기술적인 부분은 차치하고서라도 그에 대비한 관심이나 인식은 크게 개선되고 있지 않은 것 같다. 침해사고 발생 시점에서는 언론이나 주요 전문가들에 의해서 이슈화가 되고 주목을 받지만 그 시기가 좀 지나면 그에 대한 관심도는 현저히 줄어드는 것 같다. 따라서, 네트워크화된 사회에서 그 순기능을 최대한 활용하기 위해서는 단편적인 침해사고 개개의 것에 대한 대책 수립이 아닌 국가 차원의 방향을 제시하여 국민들의 인식을 한 차원 끌어올려 인터넷 네트워크 사회가 나아가야 할 방향성을 제시할 수 있는 종합적이고 장기적인 접근이 반드시 필요하다 할 것이다. 개인들의 정보보호에 대한 인식은 정보보호 관련 법제도의 정비와 시행 등으로 예전에 비해 많이 개선되고 있으나, 위협에 대해 상시 대비할 수 있고 안전한 네트워크 사회를 지켜내기 위해서는 정부뿐만 아니라 개개인의 노력 또한 필요하다.

Ⅱ. 최근 10여 년간 발생한 주요 인터넷 침해사고

1. 1.25 인터넷 침해사고('03년)

2003년 1월 25일 오후 2시경 미국, 호주 등 해외로부터 유입된 슬래머 웜(Slammer Worm)이 초당 1만 ~ 5만개의 패킷(404 Byte)을 대량 생산하여 네트워크를 공격함으로써 KT가 운영하는 국제 관문국1)인 서울 혜화전화국의 도메인네임시스템 서버가 엄청난 양의 데이터 트래픽을 이기지 못하고 처리 속도가 급격히 떨어지는 등 심각한 병목현상이 발생하였고, 이로 인해 외국으로의 인터넷 접속장애 및 국내 DNS서버에 과부하를 초래하여 인터넷이 중단된 사고이다.

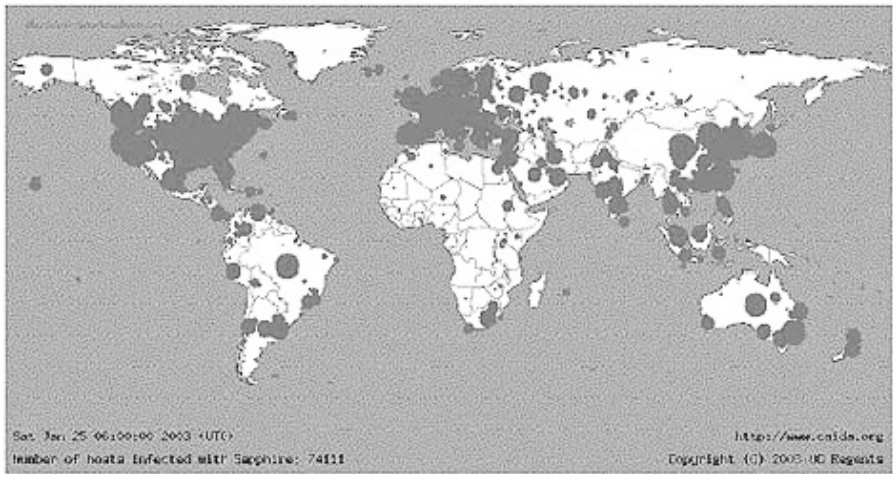
1.25 인터넷 침해사고를 유발한 슬래머웜은 UDP(User Datagram Protocol) 1434 포트를 통해 전파되는 404 바이트 크기의 메모리 상주형 웜으로서 2002년 7월 24일 공표된 'Microsoft SQL 서버 2000 및 MSDE 2000 시스템의 버퍼 오버프로우 취약점'을 이용하여 전파되었으며, MS-SQL 서버 2000 및 MSDE 2000 시스템 중 상기 취약점에 대한 보안패치를 적용하지 않은 서버 중 외부로부터 UDP 1434 포트에 대한 접근이 가능한 경우에 감염되었다. 특히, 슬래머웜은 UDP 특성을 이용해 공격을 감행하므로 확산속도가 매우 빨랐던 것으로 보고되었다. 이 당시 슬래머웜이 야기한 피해현황을 살펴보면, 미국의 산 · 학 · 연 · 관 협업 연구기관인 CAIDA(The Cooperative Association for Internet Data Analysis)의 발표에 따르면, 전세계 'Microsoft SQL 서버 2000' 중 취약점 업데이트를(패치 업데이트) 하지 않은 서버의 90%가 10분 이내에 감염되었다고 보고하였으며, 국내에서는 전 세계 감염시스템(약 7만 5천 개)의 11.8%인 8천 8백여 개가 감염되어 일본의 약 7배, 중국의 약 2배에 달하는 것으로 보고되었다. 주요 국가별 피해규모는 아래 표 1과 같다.

〈표 1〉 주요 국가별 감염시스템 수

구분	한국	미국	중국	일본
감염시스템 수 (전세계 감염서버 대비 비율)	8,848 (11.82%)	32,091 (42.87%)	4,708 (6.29%)	1,288 (1.72%)

1) 해외로 통하는 인터넷 트래픽을 통제하는 곳

전문가들에 따르면 1.25 인터넷 침해사고에 따른 전 세계적인 슬래머웜으로 인한 피해규모를 금액으로 환산하면 약 12억 달러에 이를 것으로 추정하고 있다.



[그림 1] 슬래머웜 확산 30분간 감염분포(출처 : CAIDA)

또한, 슬래머웜이 야기한 국외 피해현황의 일부를 구체적으로 살펴보면 다음 표 2와 같다.

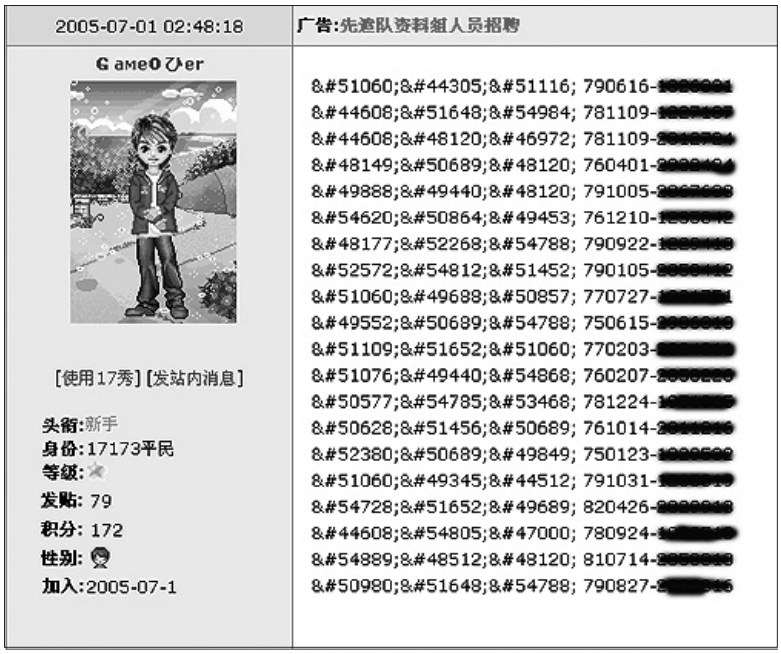
〈표 2〉 1.25 인터넷 침해사고 슬래머웜에 의한 국외 피해 사례

피해 업체	피해 사례
뱅크 오브 아메리카	- 토요일에 상당수의 현금인출기의 사용 불능상태 야기 및 금융서비스 일부 피해
컨티넨탈 항공	- 온라인 티켓팅 및 체크인 문제가 발생 - 일부 항공 스케줄이 연착 및 취소
MS	- 윈도우 XP가 동작하지 않아 게이머들은 애셔론의 콜2 서버에 접속할 수 없음 - MS의 네트워크 접속률 저하
시애틀	- 911 응급연락망 다운
워싱턴상호금융	- 월요일까지 현금인출기 사용 불가 - 금융 서비스 일부 피해
W3 인터네셔널 미디어	- 운영 중인 수천개의 웹 사이트 서버가 6시간 동안 중단
캐나다임페리얼은행	- 현금자동인출기의 시스템이 일부 마비

출처 : 1.25 인터넷 대란의 원인분석, 국가보안기술연구소, 김은영, 박중길, 재인용

2. 리니지게임 명의도용 사고('06년)

2005년 9월경 중국에서 우리나라 국민들의 주민등록번호를 도용하여 약 5만개의 리니지 게임 계정을 불법적으로 만들어 판매하는 1차 명의 도용 사태가 발생하였고, 2006년 2월경 중국에서 우회접속 IP를 이용하여 우리 국민의 명의와 주민등록번호를 도용하여 21만여 개의 개정을 개설한 2차 명의 도용 사건이 언론을 통해 알려지게 되었다. 우리 국민들의 주민등록번호 명의 도용 사건은 일견 예견되던 일이기도 했다. 우리나라 특유의 온라인 인증 수단으로써의 무분별한 주민등록번호의 사용과 온라인상에서 공공연하게 거래되고 있던 주민등록번호 등 관행적으로 묻어두던 문제가 리니지게임 명의도용 사건을 통해서 대국민 경각심을 일으킨 사건이라 할 수 있다. 중국 온라인 사이트에서 노출되고 있는 우리 국민들의 주민등록번호의 예를 보면 아래 그림 2와 같다.



[그림 2] 우리 국민의 주민등록번호가 노출된 중국 온라인 사이트(출처 : 월간 네트워커)

특히, 중국에서는 게임 아이템의 현금 거래를 통해 돈을 벌기 위해 조직적으로 명의를 도용하는 등 게임 아이템 거래를 전문적으로 하는 작업장이 성행하여 우리 국민들의

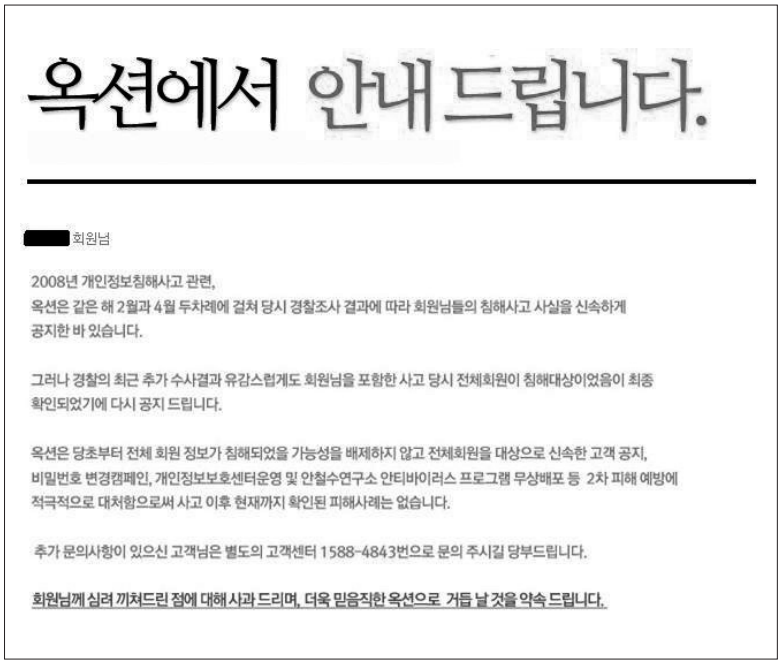
주민등록번호가 주요 타깃이 되었다. 이는 또한 간단한 인터넷 검색만으로도 우리 국민들의 주민등록번호가 쉽게 검색되고 우리 인터넷 문화의 특성상 개인인증을 위한 대부분의 수단으로써의 주민등록번호 남용에 기인한 것으로도 볼 수 있다.

리니지 게임 명의도용 사건 보도 후 도용 피해자들의 수는 기하급수적으로 늘어났으며, 명의도용 피해를 본 개인들 1만 여명이 모여 리니지 제작사인 엔씨소프트와 대표를 상대로 손해배상 청구소송을 제기했으나 법원에서는 "제작사의 이용약관과 관련법령을 봤을 때 회사가 회원가입 때 본인을 확인해야 할 의무가 없다"면서 "회사는 원고들의 명의를 도용한 사람들과 직접 관련이 없는 간접적인 제3자에 불과해 원고들의 손해를 배상할 의무가 있다고 보기 어렵다"고 밝히고, "명의도용 범죄발생 후 이뤄진 후속조치 등을 종합하면 회사가 명의도용 행위에 대해 주의의무를 다했다고 보인다"면서 명의 도용 사건과 관련하여 제작사의 책임이 없다고 판결하면서 사건은 일단락 되었다.

3. 옥션 해킹사고('08년)

2008년 1월경 중국인으로 추정되는 해커가 4차례에 걸쳐 옥션의 웹 서버 중 하나인 이노믹스 서버에 침입하여 이노믹스 서버를 통해 옥션의 메인디비2(MAINDB2) 데이터베이스 서버에 저장되어 있던 옥션 회원의 이름, 주민등록번호, 주소, 전화번호, 아이디, 계좌번호 등 개인정보를 자신의 컴퓨터로 내려받아 유출했다. 이 당시 유출된 개인정보 건수는 회원 전체인 10,807,471명의 개인정보로 이는 당시까지 발생한 개인정보 유출 사고 중 최대 규모로 사회적 파문을 야기했다. 구체적인 해킹 경로를 살펴보면, 옥션이 운영하는 아이디 'admin', 비밀번호는 기본으로 설정되어 있는 톰캣 서버에 무단 로그인한 다음 위 서버에 백도어 프로그램을 올렸고 이후 'ipconfig' 등의 명령어를 실행하여 IP 주소 등 시스템 정보를 획득하여, 3389 포트의 터미널 서비스를 기동한 다음, 자신의 IP 주소를 세탁하기 위하여 한국 내 경유지로 터미널 서비스 포트를 포워딩했다. 이어서 경유지인 서버를 거쳐 옥션의 이노믹스 서버를 통하여 데이터베이스 서버에 접속한 다음 데이터베이스 서버에 저장되어 있던 옥션 회원의 개인정보를 경유지로 전송하고, 경유지에서 개인정보를 백업한 다음 자신의 컴퓨터로 전송받은 것이었다.[2)]

2) 보안뉴스, '[정보보호법바로알기 48] 개인정보 관련 10대 집단소송 사례' 중 옥션 해킹 사건 재인용



옥션에서 안내드립니다.

[redacted]회원님

2008년 개인정보침해사고 관련,
옥션은 같은 해 2월과 4월 두차례에 걸쳐 당시 경찰조사 결과에 따라 회원님들의 침해사고 사실을 신속하게 공지한 바 있습니다.

그러나 경찰의 최근 추가 수사결과 유감스럽게도 회원님을 포함한 사고 당시 전체회원이 침해대상이었음이 최종 확인되었기에 다시 공지 드립니다.

옥션은 당초부터 전체 회원 정보가 침해되었을 가능성을 배제하지 않고 전체회원을 대상으로 신속한 고객 공지, 비밀번호 변경캠페인, 개인정보보호센터운영 및 안철수연구소 안티바이러스 프로그램 무상배포 등 2차 피해 예방에 적극적으로 대처함으로써 사고 이후 현재까지 확인된 피해사례는 없습니다.

추가 문의사항이 있으신 고객님은 별도의 고객센터 1588-4843번으로 문의 주시길 당부드립니다.

회원님께 심려 끼쳐드린 점에 대해 사과 드리며, 더욱 믿음직한 옥션으로 거듭 날 것을 약속 드립니다.

[그림 3] 옥션 해킹사고 안내문(블로그 가눔의 일상다반사)

한편, 옥션 해킹사건의 피해자들은 옥션과 이 회사의 보안관제 업체를 상대로 손해배상 청구소송을 제기하였으나, 법원은 해킹 방지 의무를 위반한 경우 개인정보도난의 책임을 물게 할 수 있는데, 해킹 사고 당시 서버에 대한 보안조치를 소홀히 했다고 볼 수 없다고 판결하였다. 옥션 해킹사건 이후 국내 주요 개인정보 유출사고 발생 현황을 보면 아래 표 3과 같다.

〈표 3〉 국내 주요 개인정보 유출사고 현황 (단위 : 명)

사건	유출인원	시기
KT	870만	2012년 7월
EBS	400만	2012년 4월
메이플스토리	1,320만	2011년 11월
네이 · 싸이월드	3,500만	2011년 7월
현대캐피탈	175만	2011년 4월
신세계몰	330만	2010년 3월
GS칼텍스	1,125만	2009년 9월
옥션	1,860만	2008년 2월

4. 7.7 DDoS 공격('09년)

2009년 7월 5일 미국의 21개 주요 정부기관, 금융, 인터넷 포털 사이트를 대상으로 한 대규모 DDoS 공격을 시작으로 7월 10일까지 총 4차례에 걸쳐 미국 및 국내 주요 정부기관, 금융기관 및 인터넷 포털 사이트를 대상으로 DDoS 공격이 발생하였다. 우리나라의 경우에는 7월 7일부터 10일까지 총 3차례에 걸친 DDoS 공격으로 청와대 등 주요 정부기관과 인터넷 사이트가 마비되는 사건이 발생하게 되었다. 국내외 DDoS 사건의 경과를 살펴보면 다음의 표 4와 같다.

〈표 4〉 7.7 DDoS 사건 기간별 경과사항

구분	기간	주요 공격대상
1차 DDoS 공격	2009.7.5.~6	미국 21개 주요 정부기관, 금융, 인터넷사이트 등 대규모 공격 발생
2차 DDoS 공격	2009.7.7~8	국내 12개, 미국 14개 주요 정부기관, 금융, 인터넷사이트 등 대규모 공격 발생
3차 DDoS 공격	2009.7.8~9	국내 15개, 미국 1개 주요 정부기관, 금융, 인터넷사이트 등 대규모 공격 발생
4차 DDoS 공격	2009.7.9~10	국내 7개 주요 정부기관, 금융, 인터넷사이트 등 대규모 공격 발생

출처 : Cisco Systems Korea, 2009.7.16

또한, 국내 공격대상 기관을 구체적으로 살펴보면, 아래 표 5와 같다.

〈표 5〉 7.7 DDoS 국내 공격 대상 기관

기관유형	공격 진행 시간 (7월 7일 18시 ~ 7월 10일 18시)		
	24시간	48시간	72시간
공공기관	국회, 한나라당, 외교통상부, 국가정보원, 행정안전부	청와대, 국방부, 한미연합사령부	-
언론	-	-	조선닷컴
기업	안철수연구소, 이스트소프트	다음 , 파란	네이버, 옥션
은행	외환은행, 신한은행, 농협, 우리은행, 하나은행, 기업은행	국민은행	-

출처 : 현안참고자료, 현대경제연구원, 2009.7.23

7.7 디도스 사건은 기존의 디도스 공격과는 다른 양상을 보였다. 즉 기존의 디도스 공격에서는 좀비 PC를 실시간으로 단순 조정하여 공격하였으나, 7.7 디도스의 경우에는 악성코드의 기능 및

공격대상을 업데이트 할 수 있는 숙주서버에 특정시간에 일정 주기로 접속해 공격대상 및 공격시간 스케줄링 명령을 받게 하여 공격대상과 공격시간을 명령받은 십만대 이상의 좀비PC가 이미 정해진 명령에 따라 공격대상 웹사이트를 동시에 공격하였다. 또한, 공격에 사용된 좀비PC의 악성코드는 감염 경로를 추적할 만한 정보를 모두 제거한 진화된 형태의 공격이 이루어졌다. 한편 기존 디도스 공격이 금전적 목적으로 이루어진대 반해 7.7 디도스는 정부, 금융, 포털 등 사회적 혼란을 야기할 목적으로 수행된 것으로 추정되어 향후 디도스 공격의 변화양상을 엿볼 수 있는 사건이라 할만하다. 즉 이후 인터넷 침해사고의 양상이 사이버 테러의 한 방편으로 활용되고 있음을 알 수 있다. 기존의 디도스 공격과 7.7 디도스 공격을 비교하면 아래 표 6과 같다.

〈표 6〉 기존 디도스 공격과 7.7 디도스 공격 양상 비교

구분	기존 디도스 공격	7.7 디도스 공격
명령 · 제어서버 존재여부	해커로부터 명령을 받는 명령 · 제어 서버 존재	악성코드를 업데이트하는 서버 존재
공격 방법	명령 · 제어 서버의 네트워크를 통한 실시간 공격 제어	일정 주기로 악성코드를 업데이트 받아 스케줄링을 통한 공격
감염 경로	윈도우즈 또는 브라우저 취약점을 악용한 홈페이지 악성코드로 인한 감염	공격자가 정상적인 프로그램에 숨겨둔 악성코드가 동작
방어 방법	명령 · 제어 서버 차단	공격 PC의 악성코드 제거
공격 대상	홈페이지 1~2개	다수 홈페이지에 동시 다발 공격
악성코드 갯수	디도스 공격을 수행하는 악성코드 1개 다운로드	압축파일 형태의 악성코드를 다운로드, 디도스 공격 외에도 다양한 악성행위 수행 네트워크 연결정보
네트워크 연결정보	평문 채널을 통한 통신으로 공격명령 내용 모니터링 가능	암호화된 채널을 사용하여 통신하므로 통신내용 확인 불가
악성 행위	해커의 명령을 지속적 수행	단기공격 수행 후 하드디스크 삭제
공격 목적	금전적 이득	사회혼란 유발(추정)
공격 주체	주로 중국 등에 위치한 해커 조직	미확인

출처 : 7.7 DDoS 공격, "어떤 사건이었나?, 보안뉴스, 2010.7.7

5. 3.4 디도스 대란('11년)

2011년 3월 3일 오후 5시경 최초로 국내 포털 사이트 및 공공기관의 웹 사이트에 대한 공격 징후가 발생하였고, 이후 4일 오전 10시와 오후 6시 30분 사이 국방, 은행, 인터넷 포털, 공공기관

등 총 40개의 웹사이트를 대상으로 디도스 공격이 발생하였다. 구체적인 공격 대상 웹 사이트를 살펴보면 아래 표 7과 같다.

〈표 7〉 3.4 DDoS 공격 대상 기관

기관유형	공격 진행 시간	
	1차 공격(3월 4일 오전 10시)	2차 공격(3월 4일 오후 6시 30분)
공 공	경찰청, 국가대표포털(korea.go.kr), 국세청, 국회, 통일부, 청와대, 외교통상부, 한국인터넷진흥원, 행정안전부, 금융위원회,	경찰청, 국가대표포털(korea.go.kr), 국세청, 국회, 금융위원회, 관세청, 외교통상부, 청와대, 통일부, 한국인터넷진흥원, 행정안전부, 국가정보원, 방송통신위원회, 한국수력원자력, 한국철도공사
국방	공군본부, 국방부, 방위사업청, 육군본부, 주한미군, 합동참모본부, 해군본부	공군본부, 국방부, 방위사업청, 육군본부, 주한미군, 합동참모본부, 해군본부, 국방홍보원, 미8군 전투비행단
민간	네이버, 다음, 디시인사이드, 안철수연구소, 지마켓, 한게임	네이버, 다음, 디시인사이드, 안철수연구소, 지마켓, 한게임, 옥션
은행	국민은행, 농협, 대신증권, 신한은행, 외환은행, 키움증권	국민은행, 농협, 대신증권, 신한은행, 외환은행, 키움증권, 우리은행, 제일저축은행, 하나은행

3.4 디도스 대란은 지난 2009년 7.7 디도스 사건 후 2여 년 만의 일로 그 당시와 유사한 패턴을 보였지만 한층 업그래이드된 모습을 보였다. 안랩에 따르면, 7.7 디도스 공격에서는 같은 파일 구성으로 여러 차례 공격했으나 3.4 디도스 공격에서는 공격 때마다 파일 구성이 달라지고 새로운 파일이 추가 제작되어 활용되었으며, 손상 운영체제도 기존에는 닷넷 프레임웍 기반인 윈도 2000/XP/2003에 국한됐으나, 3.4 디도스 공격에서는 모든 윈도우 운영체제가 타깃이 되는 등 여러 차이점을 보였다고 한다. 7.7 디도스 공격과 3.4 디도스 공격을 차이점을 구체적으로 살펴보면 아래 표 8과 같다.

〈표 8〉 기존 디도스 공격과 7.7 디도스 공격 양상 비교

구분	7.7 디도스 공격('09년 7월 7일)	3.4 디도스 공격('11년 3월 4일)
공격대상	청와대 등 국내 주요 사이트 23곳	청와대 등 정부사이트, 주한 민군 등 40곳
공격지속기간	7~9일 3일간 오후 6시에서 다음날 6시까지	3일 오후 이상 징후 발생, 4일 오전 10시, 오후 6시 30분에 시작, 공격종료 시점 불확실
손상 운영체제	닷넷 프레임웍 기반 윈도우 2000/XP/2003	모든 윈도우 운영체제
파일 구성	같은 파일 구성으로 여러 차례 공격	공격때마다 파일구성이 달라짐
명령 변경	변경 없이 일관되게 진행	대응에 따라 명령을 변경함

치료 방해	없음	호스트 변조로 백신 업데이트 및 홈페이지 접근 방해
하드디스크 및 파일 손상 시점	마지막 디도스 공격 날인 10일 자정 손상 당시 백신을 설치하지 않은 PC는 시스템 날짜를 이전으로 바꿔야 했음	시스템 날짜를 감영 시각 이전으로 바꾸거나 감염 시각을 기록한 noise03.dat 파일을 삭제할 경우 감염 후 7일, 4일 후로 계획했다가 5일 밤 9시경을 기해 즉시 손상되는 것으로 변경
좀비PC수 (방통위 발표)	115,044대	116,299대
대응방식	제대로 준비되지 않은 상태에서 대대적 혼란 야기	7.7 디도스 이후 기업/기관의 준비가 있었고, 보안 업체와 유관 기관과의 협조로 피해 최소화

출처 : 3.4 DDoS 분석보고서, 안랩, 2011.3.

한편, 3.4 디도스 사건의 경우 7.7 디도스 공격 당시 보다 공격 대상 및 규모도 늘어나고 공격에 이용된 악성코드도 보다 지능적이었지만, 실질적인 피해는 그리 크지 않았던 것으로 나타났다. 이와 관련하여 정부에서는 7.7 디도스 사건의 학습효과와 경험을 토대로 각 정부기관의 대응기능을 명확히 하고 대국민 언론 홍보 기능을 일원화 하는 등 대응체계를 정립하고 디도스 대응장비 구축 · 확충 등의 정보보호 투자를 대폭 늘렸기 때문이라고 평가했다. 또한 민간에서도 디도스 대응 투자를 증액하고 대응인력을 보강하는 등 사전적 대비를 한층 강화한 것도 큰 기여를 했다. 더불어 정부와 민간기관이 정보를 공유하고 상호 협력하여 발 빠른 대응을 함으로써 피해를 크게 줄일 수 있었다고 평가하였다.

6. SK컴즈 개인정보 유출사고('11년)

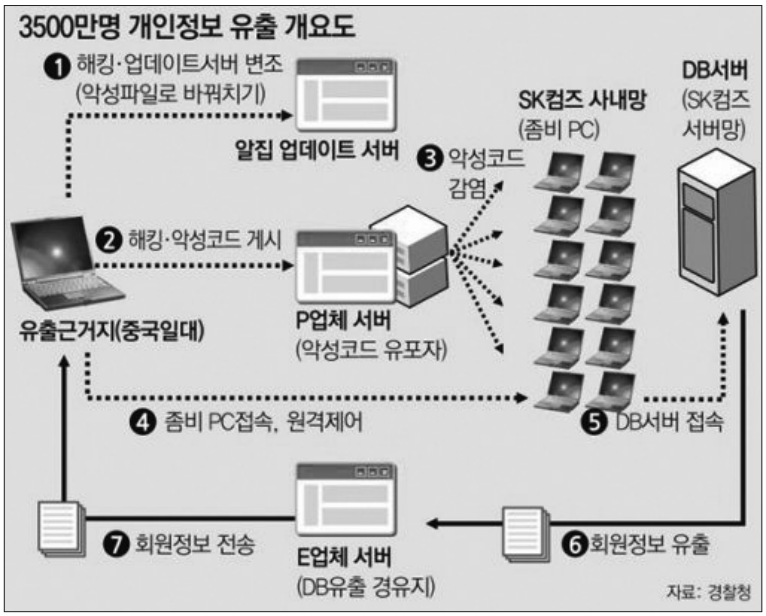
2011년 7월 26일에 네이트의 데이터베이스에 저장된 가입자 3,500만 명 전원의 아이디, 비밀번호, 이름, 주민등록번호, 연락처 등의 개인정보가 유출된 사건으로 사상 최대 규모의 개인정보 유출 사건으로 기록되었다. SK컴즈 개인정보 유출사건의 주요 경과 사항을 살펴보면 다음 표 9와 같다.

〈표 9〉 SK컴즈 개인정보 유출 일지

일시	내용
7월 19일	알집 업데이트 서버 해킹
7월 25일	내부 접속정보 추가수집
7월 26일	3,500 만명 개인정보 유출
7월 28일	SK컴즈 개인정보 유출 확인
7월 29일	SK컴즈 유출사태 기자회견

출처 : 한국인터넷진흥원 내부자료

경찰의 SK컴즈 수사결과를 살펴보면 이스트소프트의 공개용 알집 업데이트 서버가 해킹당해 정상 업데이트 파일을 악성파일로 바꿔치기한 수법이 사용됐다는 결론을 내렸다. 즉 해커들이 이스트소프트의 알집 업데이트 서버를 해킹하여 일반 이용자들이 업데이트를 실행하면 알집을 통해 해킹프로그램이 설치되도록 하였고, SK컴즈 직원들 역시 알집 업데이트를 통해 이에 감염되면서 관리자 계정이 해킹당하면서 사상 초유의 개인정보 유출이 발생하게 된 것이다. 경찰청 사이버테러대응센터는 SK컴즈, 이스트소프트 등 관련 업체의 PC와 서버 40여대를 분석한 결과 이 사건의 진원지로 중국을 지목하였다. 경찰청이 발표한 이번 사건의 흐름을 보면 아래 그림 4와 같다.



[그림 4] SK컴즈 개인정보유출 사건 개요(출처 : 동아닷컴)

SK컴즈 개인정보유출 사고의 피해자들은 사건 이후 집단소송 등 여러 손해배상 소송을 제기하였으니 법원의 판결은 엇갈리고 있다. 2012년 11월 피해자 2,847명이 서울중앙지법에 제기한 소송에서는 원고 패소 판결이 내려졌고, 피해자 2,737명이 서울서부지법에 제기한 민사소송에서는 원고에게 위자료로 각 20만원을 지급하라는 원고 승소 판결이 내려졌다. 그리고 가장 최근의 서울중앙지법 민사소송에서는 피해자 9명의 손해배상청구가 기각 및 각하 결정이 내려지는 등 판결이 엇갈리게 나타나고 있다.

7. 3.20 및 6.25 사이버 공격('13년)

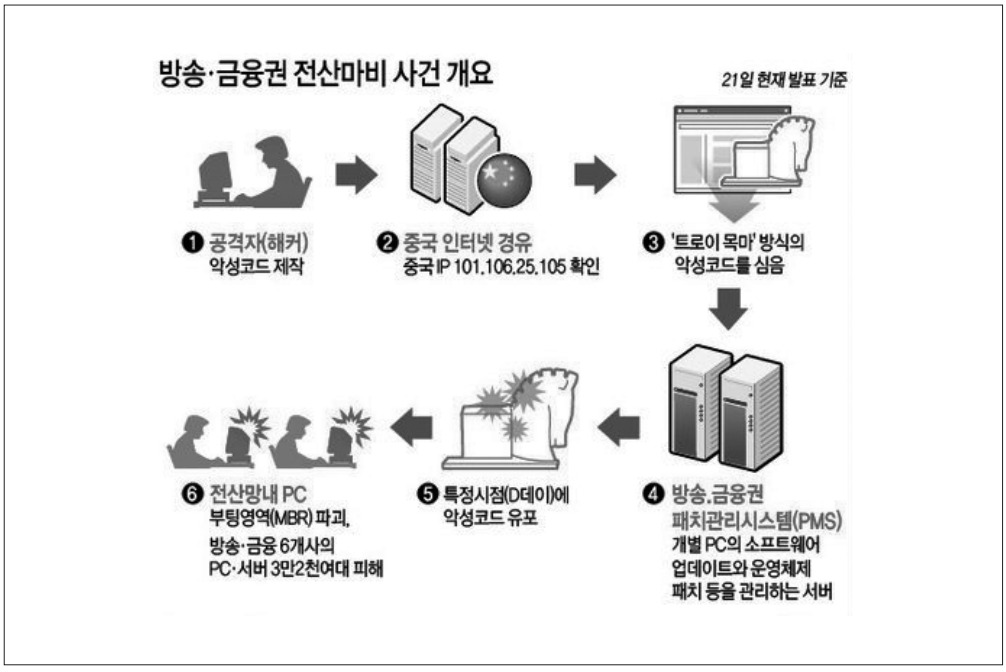
2013년 3월 20일 오후 2시 50분경 국내 주요 언론사와 금융권의 전산망이 악성코드에 감염되어 다운되는 사태가 발생하였다. 방송 및 금융부문 6개사 전산망이 동시에 마비되어 최장 10일간의 복구 기간이 소요되었다. 공격 대상 업체의 주요 피해현황을 살펴보면 아래 표 10과 같다.

〈표 10〉 3.20 사이버 공격 대상 업체의 피해현황

구분		피해 현황	복구 현황
방송사	MBC	서버 18대 PC 1,000대	복구 완료 (3.26)
	KBS	서버 6대 PC 4,000대	복구 완료 (3.21) 복구 완료 (3.26)
	YTN	서버 5대 PC 370대	복구 완료 (3.25)
금융기관	농협	CD/ATM 16,000대 PC 26,000대	복구 완료 (3.25) 복구 완료 (3.29)
	신한은행	서버 4대 PC 169대	복구 완료 (3.20)
	제주은행	CD/ATM 320대 PC 70대	복구 완료 (3.23) 복구 완료 (3.24)

출처 : 한국인터넷진흥원 내부자료

3.20 사이버 공격으로 악성코드에 감염된 PC는 마스터 부트 레코드(MBR)와 볼륨 부트 레코드(VBR)가 파괴되어 부팅되지 않았으며, 기존 데이터들이 소실되는 피해를 입었다. 주요 피해 사례를 살펴보면 KBS, MBC, YTN 등 주요 방송사와 언론사가 피해를 입었으며, 신한금융계열의 신한은행과 제주은행 전산망이 장애를 일으켰으며, 농협은행도 일부 PC에 장애가 발생하여 인터넷을 차단하는 등 피해가 발생하였다. 연합뉴스에 따르면, 3.20 사이버 공격으로 실제 피해를 입은 PC는 3만 2천여 대로 추정되며, 사실상 손상된 데이터의 원 상태로 복구하는 것이 불가능하다고 전망하였다. 이는 3.20 공격의 경우 PC의 부팅 영역만 공격한 것이 아니라 하드디스크 자체를 손상시켰기 때문에 손상된 데이터의 완전 복구는 어려울 것이다. 3.20 전산대란의 주요 진행과정을 살펴보면 아래 그림 5와 같다.



[그림 5] 3.20 사이버대란 사건 개요(블로그 다독다독)

Red Alert에서 발표한 3.20 사이버테러 사고 분석보고서에 따르면, 3.20 사이버 공격의 암호 알고리즘과 기존의 2007년에서 2011년 사이에 있었던 공격의 암호 알고리즘을 비교 분석한 결과 아래 표 11과 같이 주요 유형별 데이터 값이 동일하게 나타나, 3.20 사이버 공격이 일시적이고 갑작스런 공격이 아닌, 동일한 조직에 의한 치밀하게 준비되고 계획된 공격으로 추측된다.

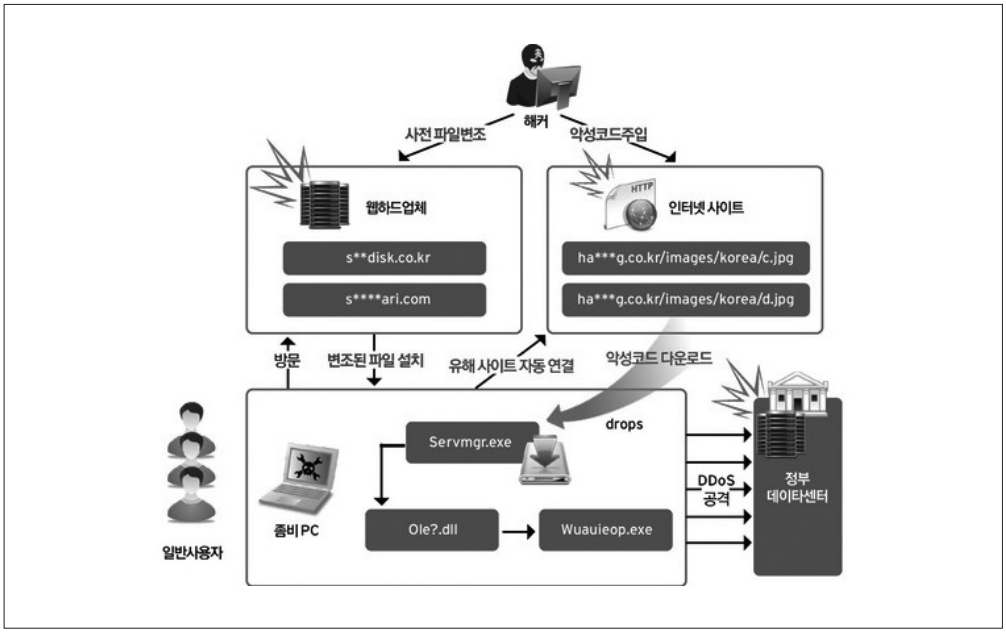
〈표 11〉 3.20 사이버 공격 및 기존 공격의 암호 알고리즘 비교

24시간	압축 암호 값	RSA키 값	C&C 프로토콜 데이터 값	Packer	XTEA키 값
2007-2011 공격	동일	동일	동일	동일	동일
3.20 사이버 공격					

출처 : 3.20 사이버테러 사고 분석보고서, Red Alert

3.20 사이버 공격의 여운이 채 가시기도 전인 2013년 6월 25일 오전 9시 10분경 청와대 홈페이지 및 주요 정부기관 등에 대한 사이버 공격이 감행되었다. 정부 발표에 따르면, 6.25

사이버 공격의 대상기관은 69개 기관으로 홈페이지 해킹 47개 사이트, 디도스 공격 8개 사이트, 악성코드 공격으로 인하여 하드디스크가 파괴된 경우가 14곳으로 나타났다. 이번 공격 또한 지난 3.20 사이버 공격의 북한의 해킹 수법과 일치하는 것으로 정부에서는 북한의 소행이라고 공식 발표했다. 정부에서는 6.25 사이버 공격의 국내 경유지에서 발견된 IP와 북한이 사용하는 IP가 동일한 점, 또한 악성코드 공격에 따른 시스템 부트영역 파괴, 시스템의 주요파일 삭제, 해킹 결과를 전달하기 위한 공격상황의 모니터링 방법, 악성코드 문자열의 특징이 3.20 사이버 공격과 동일한 점을 들어 6.25 사이버 공격 역시 북한의 소행으로 추정하였다. 6.25 사이버 공격의 전체적인 흐름을 살펴보면 아래 그림 6과 같다.



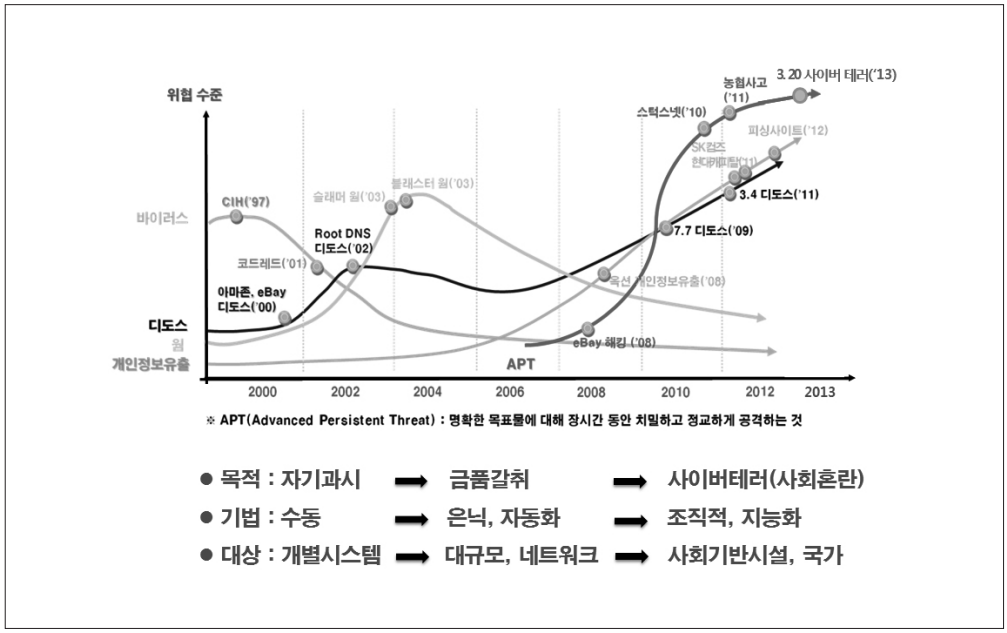
[그림 6] 6.25 사이버 공격 사건 개요(미디어잇)

Ⅳ. 시사점

지금까지 지난 10여 년간 국내에서 발생한 주요 인터넷 침해사고 및 개인정보 유출사고의 흐름을 살펴보았다. 앞서 살펴본바와 같이, 정보통신기술의 발달로 인한 사회 시스템의

네트워크화는 생산성 및 효율성 향상, 정보격차의 해소, 언제 어디서나 필요한 정보를 쉽게 얻고 가공하여 새로운 부가가치를 창출하는 등 우리 사회의 발달에 기여한 바가 매우 크다고 하겠으나, 또 한편으로는 네트워크로 연결된 사회에서의 해킹, 디도스 공격, 개인정보유출, 피싱 등의 역기능은 자칫 사회 전체를 위기로 몰아넣을 수 있는 극단적인 무기로 사용될 수 있다. 따라서, 정보통신기술이 고도화되면 될수록 그 기반이 되는 정보보호의 중요성은 아무리 강조해도 지나치지 않을 것이다.

지난 인터넷 침해사고의 흐름을 살펴보면, 디도스 및 해킹 공격은 보다 지능화되고 진화된 공격 형태를 나타내고 있으며, 단순히 금전적인 이득을 목적으로 하거나 개인의 과시욕에서 실행하는 단순한 행태에서 벗어나 점차 의도적으로 사회적 혼란을 야기하거나 정치적인 목적 달성을 위한 사이버 테러의 형태로 진화하고 있다. 이러한 인터넷 침해사고의 진화 유형을 살펴보면 아래 그림 7과 같이 요약해 볼 수 있다.



[그림 7] 인터넷 침해사고의 진화

따라서, 이러한 진화하고 발전하는 인터넷 침해사고에 적절히 대응하고, 보다 안정적이고 신뢰할 수 있는 우리 사회의 발전을 위해서는 정부차원의 장기적이고 종합적인 정보보호

대책의 수립과 더불어 사회 구성원들이 자발적으로 실천할 수 있는 방향제시가 필요하다고 생각된다. 이는 적정한 예산의 투입뿐만 아니라, 사회 모든 부문의 구성원들이 개인의 안전한 생활과 사회 전체의 발전을 위해서는 구성원 각자의 정보보호의 중요성에 대한 인식제고와 이를 실생활의 작은 것에서부터 실천하는 생활화가 중요할 것이다. 또한, 진화하는 인터넷 침해사고에 대비하기 위해서는 정부의 노력뿐만 아니라 민간 부문에서도 자율적으로 대응체계를 구축할 수 있도록 보안산업의 활성화가 필요하다. 이를 위해서는 우선적으로 적정 수준의 전문 보안 인력의 꾸준한 양성이 반드시 요구된다. 기업들이 정보보호에 대한 투자를 비용으로 생각하지 않고 과감하게 투자 할 수 있도록 여러 정책적 지원 방안을 마련하는 것도 좋은 방법일 것이다.

끝으로, 정보보호 분야는 단기간 내에 직접적이고 가시적인 효과를 볼 수 없는 특성을 가지고 있기 때문에 너무 조급하게 단기적인 성과에 급급하여 사고 시 마다 단편적인 대책을 강구하는 것에서 벗어나 정부가 주도하여 사회 모든 구성원들이 참여하여 정보보호 대응능력을 강화할 수 있는 시스템 체계를 구축함으로써 사회 안전망이 강화될 수 있도록 중장기적으로 접근하는 노력이 필요하다.

참고문헌

다독다독 블로그, "최근 사이버테러로 살펴보는 예방 수칙",
2013.3.25. 〈http://www.dadoc.or.kr/812〉

가눔의 일상다반사 블로그, "옥션 해킹사건... 알고보니 전체회원 개인정보유출", 2010.3.26.
〈http://ganum.tistory.com/entry/옥션-해킹사건알고보니-전체회원-개인정보유출〉

Red Alert, 3.20 사이버테러 사고 분석 보고서, 2013.4.19.

한국인터넷진흥원, 인터넷 침해사고 피해액 산출모형 개발에 관한 연구, 2006.12.

"6.25 사이버공격 67곳 타격... 14곳은 정보파괴", 머니투데이, 2013.7.4.

"6.25 사이버테러는 북한 소행 정부 공식 발표", 이투데이뉴스, 2013.7.16.

"6.25 사이버 공격, 취약한 웹하드 서버 관리가 원인", 미디어잇, 2013.6.27.

"사이버 테러 위협속, 보안업계 명품인재 육성 절실", 뉴스한국, 2013.8.13.

David Sancho, "SK컴즈 대형 데이터 유출 사고, 3천 5백만 사용자 정보 도난", Trend Micro, 2011.7.29.
〈http://www.etnews.com/news/telecom/public/1751419_2562.html〉

"네이트 · 싸이월드 회원 3500만명 개인정보 中유출 확인", 동아닷컴, 2011.8.12.

"경찰, SK컴즈 타깃한 신종 공격으로 결론", 이티뉴스, 2011.8.11.

"SK컴즈 시스템 감염시킨 악성코드는 10여개 달해", 이티뉴스, 2011.7.31.

"싸이월드 개인정보 유출사건 판결 계속 엇갈려", 법률신문, 2013.8.21.

"법원, 싸이월드 개인정보 유출 손배청구 기각... 자료 불충분", 아시아경제, 2013.8.21.
"SK컴즈, 개인정보 유출 20만원 배상 판결에 항소", 아시아경제, 2013.2.27
김중태, "리니지 게임의 명의도용 사태, 원인과 대책", 2006.2.17.
〈http://www.dal.kr/col/interview/20060217_KBSfm.html〉
"리니지 사태, 주민번호 남용이 가져온 필연적 결과", 월간네트워커, 2013.8.
장현준, "리니지 대량 명의도용 사태", 월간소비자, 2006.4.
"더 센 놈 온다 – 슬래머 웜은 시험판, 현실로 다가오는 제2인터넷 대란", 오마이뉴스, 2003.3.24.
"[1.25인터넷 대란] 웜바이러스로 인한 각국 피해상황", 동아닷컴, 2003.1.26.
"7.7.해킹, 1.25 인터넷 대란과 무엇이 다른가", 아시아경제, 2009.7.8.
"[1.25 인터넷 대란] 바이러스 35분 공격에 무너진 IT 한국", 동아사이언스, 2003.1.27.
"정통부 1.25인터넷 대란 원인과 대책 발표", 이티뉴스, 2003.2.19.
김은영, 박중길, "1.25 인터넷 대란의 원인 분석", 2003년 한국정보과학회 봄 학술발표논문집 Vol. 30, No. 1
"개인정보 관련 10대 집단소송 사례2", 보안뉴스, 2013.8.8.
"역대 최악의 해킹 사례는? 옥션 개인정보 유출", 연합뉴스, 2009.7.8.
"피해입은 3만2천대 PC 복구 난항... 포맷해야", 연합뉴스, 2013.3.21.
"[7.7DDoS 1년] 7.7 DDoS 공격, 어떤 사건이었나", 보안뉴스, 2010.7.7.
김병탁, "7.7 대란 DDoS 공격실태와 현황", 지디넷코리아, 2009.7.29.
박용규, "사이버대피소를 통해 본 12년도 DDoS 공격동향 분석",
Internet & Security Focus 2013, 2월호. 2013.2.
"7.7 DDoS 공격을 되짚어보며...", 보안뉴스, 2010.7.24.
㈜안철수연구소, 3.4 DDoS 분석보고서, 2011.3.
하우리, 3.3 DDoS 공격 분석 보고서, 2011.3.