主題

국내 인터넷 해킹실태 및 사례 분석

한국정보보호센터 정현철, 임채호

차 례

I. 서 론

21세기를 지식정보사회라고들 한다. 정보를 많이 가진 사람이 곧 부(富)와 권력(勸力)을 쟁취할 수 있는 사회이다. 이러한 지식정보사회는 인터넷을 근간으로 하는 정보인프라에 의해 이루어질 수 있다. TCP/IP를 이용한 인터네트워킹이 30여년의 짧은 역사에도 불구하고 현재에는 인터넷이라는 거대한 정보인프라로 세계가 하나로 묶여졌다. 인터넷을 근간으로 하는 사이버 공간에서는 실제 세계와 마찬가지로 모든 일들이 이루어지고 있다. 은행에 직접 찾지 않고도 거래할 수 있는 인터넷 뱅킹, 집에서 대학의 수업을 수강할 수 있는 가상대학, 정부에서 추진중인 전자정부, 시장에서 흥정하지 않고도 필요한 물건을 구매할 수 있는 전자상거래 등 이제 현실세계에서 일어나는 대부분의 일들이 가상세계로 옮겨가고 있다.

정보화의 진전에 따라 국민들의 정보수집이나 또 다른 부의 창출이 쉬워진 반면 정보화와 더불어 달갑지 않은 역기능 또한 증가하고 있는 실정이다. 이러한 정보화 역기능 중의 대표적인 것이 해킹이라고 할 수 있다. 해킹으로 인해 사이버 공간에서 자신의 얼굴이라고 할 수 있는 홈페이지가 옴탄물로 뒤범벅이 되어 버리고, 소중한 개인정보가 불법적으로 유출되기도 하고, 정상적인 인터넷 서비스를 방해하는 행위가 발생되기도 하는 등 다양한 형태의 피해가 발생되고 있다.

지식정보사회라고 일컬어지는 새천년의 시작과 함께 해킹은 전세계를 떠들썩하게 하였다. 1월 말경 일본 정부기관의 홈페이지가 연이어 해킹당하여 포르노물로 뒤바뀌어 버리거나 일본인들을 비난하는 글이 게시되기도 하였으며, 2월 7일 세계적으로 유명한 인터넷 사이트인 야후가 해킹으로 인해 수시간 동안 서비스가 중단되는 것을 시작으로 아마존, CNN, 이베이 등 세계 유수의 인터넷 사이트들이 연이어 해킹을 당하여 서비스가 마비되거나 지연되

었다.

<유명사이트 해킹 피해 일지>

2. 7	www.yahoo.com	3시간 서비스중단
2. 8	www.buy.com	4시간 동안 판매 지연
	www.ebay.com	반나절 동안 중단
	www.amazon.com	1시간 동안 판매 지연
	www.cnn.com	2시간 동안 뉴스 방해
2. 9	www.datek.com	1시간 동안 중지
	www.etrade.com	2시간 동안 중지
	www.zdnet.com	수시간 중지

그러면 외국이 이처럼 해킹으로 인해 많은 피해를 입고 있는데 국내의 경우는 어떨까. 물론 국내도 외국과 마찬가지로 수많은 해킹피해를 입고 있다. 국내의 경우 해킹에 대한 대비책이 정보화가 일찍부터 이루어진 선진 외국에 비해 뒤떨어져 더 많은 피해를 당하고 있는 실정이다. 최근 몇 년 동안 범국가적으로 지식정보사회의 기치를 내걸고 정보화를 추진한 결과 세계 10위 권내에 드는 인터넷 강국으로 자리매김할 수 있었다. 하지만 국내의 정보화는 외형만 불리는데 급급하여 실제 서비스의 질이나 보안관리 측면에서는 대단히 부족한 형편이다. 종종 국외 유명 보안관련 인터넷 사이트에서 한국의 인터넷 보안이 허술하다는 내용의 글들이 올라오곤 하는데 지식정보사회를 외치고 있는 우리나라가 이런 말들을 들어야 한다는 것이 부끄럽기도 하다. 하지만 이는 현실이다. 통신, 운송, 국방, 금융 등 국가 주요 기반시설이 정보시스템에 의존하고 있는 이때 부실 공사로 인한 삼풍 백화점 붕괴 사건의 악몽을 사이버 공간에서 다시 당하지 않도록 좀더 많은 노력과 대책이 필요하리라 생각한다.

본 고의 제2장에서는 한국정보보호센터 CERTCC-KR(Korea Computer Emergency Response Team Coordination Center)에 접수된 해킹사고를 통하여 국내 해킹 실태 및 문제점을 살펴보고 제3장에서는 몇 개의 실제 해킹사례를 통하여 해킹사고에 사용되고 있는 해킹기술을 분석하고 그 대응방안에 대해 살펴보도록 하고 4장에서 결론을 짓도록 한다.

Ⅱ. 국내 해킹 실태 및 문제점

국내 인터넷 사용자의 폭발적인 증가와 함께 국내 해킹사고도 매년 큰폭으로 증가하고 있다. 1997년도의 국내 인터넷 이용자 수가 1백 6십만명이던 것이 그로부터 2년 후인 1999년도에 1천 8십만명으로 거의 7배 가까이 증가하였다[5]. 국내 인터넷 사용자의 증가와 유사하게 해킹사고도 큰 폭으로 증가하고 있는데 '97년 64건에서 '99년 572건으로 거의 9배에 이러는 증가를 보이고 있다[1].

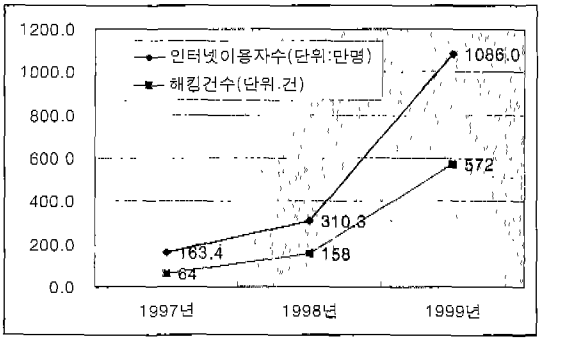

그림 1. 인터넷이용자수와 해킹건수

(그림 1)에서 보이는 것처럼 최근 몇 년 동안의 인터넷 이용자수의 증가율과 해킹건수의 증가율은 비례하는 것을 알 수 있다. 2000년 말까지 국내 인터넷 사용자가 2,000만명을 상회할 것이라고 예측하고 있는데 이와 더불어 국내 해킹사고도 큰 폭으로 증가하여 1,000건 이상의 해킹사고가 발생할 것으로 예측하고 있다. 실제 이미 2000년 2월까지 접수된 해킹사고가 221건으로 이 예측이 빗나가지 않고 있음을 알 수 있다.

이러한 현상은 국외의 경우도 마찬가지로 정보화가 추진된 정도에 비례하여 해킹사고 또한 많이 발생되고 있음을 알 수 있다. (그림 2)는 미국, 영국, 일본의 최근 3년간 해킹사고 발생 건수이다[1,9,10, 11].

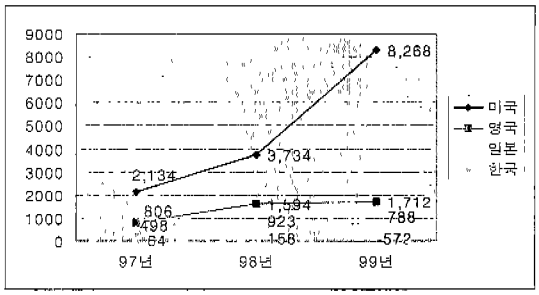

그림 2. 국외 해킹사고 증가 추이

기관별 해킹 피해 접수현황을 살펴보면 대학이 262건(45.8%)으로 가장 많은 해킹사고가 접수되었으며 일반기업이 248건(43.4%)으로 두 번째로 많은 사고가 접수되었고, 지역 등의 기타가 29건(5.1%), 비영리기관이 22건(3.8%), 연구소가 11건(1.9%) 순으로 접수되었다.

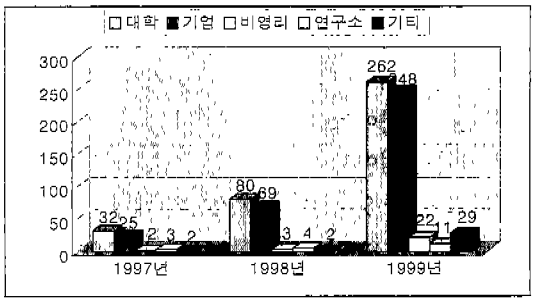

그림 3. 기관별 해킹사고 현황

대학은 많은 정보시스템이 존재하고 정보시스템 사용자도 교수, 교직원, 학생 등으로 대단히 다양하다. 대학의 개방된 환경으로 인해 해킹에 쉽게 노출될 수 있다. 접수된 대학의 해킹사고는 학과 연구실의 실험용 리눅스에서 많이 발생되었는데 학생들에 의해 개인적으로 관리되고 있었으며 비전산학과의 경우 시스템 보안관리가 전혀 이루어지고 있지 않았다. 대학 해킹사고에 대응하기 위해 학교 네트워크 관리자에 의한 중앙에서의 보안관리가 필요하다.

대학과 마찬가지로 일반기업의 해킹사고도 전체 해킹사고에서 많은 부분을 차지하고 있는데 최근 전자상거래 등을 목적으로 인터넷 사이트를 개설하는 기업이 많아 기업의 해킹사고가 꾸준히 늘어나고 있다. 일반기업의 해킹사고는 보안인력 및 보안의 기술적인 대책을 가진 대규모의 기업보다는 보안에 대한 여력이 없는 중소규모의 기업에서 많이 발생되고 있다. 최근 소자본의 인터넷 전자상거래 업체들이 하루가 다르게 늘어가고 있는데 이러한 사이트들의 해킹으로 인해 개인정보가 유출되지나 않을까하고 우려된다. 한국정보보호센터에서 전자상거래 사용자를 대상으로 실시한 설문조사 결과 인터넷 보안은 전자상거래 구축에 있어 필수사항임을 알 수 있다.

(그림 4)는 전자상거래시 해킹 등의 피해를 미연에 방지하기 위해 어떻게 대처할 것인가에 대한 설문조사 결과이다[4].

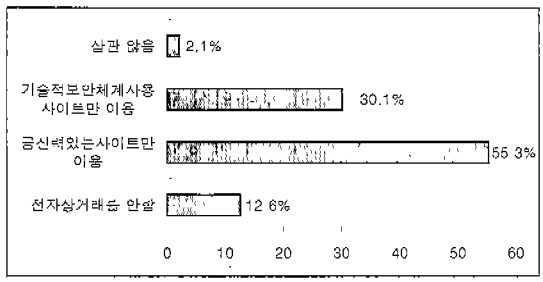

그림 4. 전자상거래 피해방지 방안

대학이나 일반기업 이외에도 비영리 단체, 연구소 등 인터넷에 연결되어 있는 시스템이라면 어느 기관을 막론하고 해킹을 당할 수 있다. 최근에는 서버급 운영체제인 유닉스 시스템뿐만 아니라 개인 PC의 윈도우즈 시스템에 대한 해킹사고가 많이 접수되고 있는데 이는 해킹이 일반 가정이나 회사를 막론하고

누구나 당할 수 있음을 시사하고 있다. 지난 한해 보고된 해킹사고가 572건이지만 실제 발생된 전체 해킹건수는 이보다 훨씬 많을 것으로 보인다.

국내와 국제간의 피해관계를 살펴보면 국내에서 국외로의 해킹시도 및 공격은 24건(4.0%)인데 반해 국외에서 국내 시스템에 대한 해킹시도 및 공격은 모두 274건(45.3%)에 달하고 있다.

표 1. 국내 국제간의 피해관계

	국내->국내	국내->국외	국외 -> 국내		미확인	계
			국외->국내	국외->국내->국외		
건수	48	24	91	183	250	596
비율 (%)	8.1	4.0	15.3	30.7	41.9	100

피해 경로를 분석할 수 없는 경우는 공격자가 추적을 피하기 위해 로그를 삭제하거나 서비스거부 공격과 같이 해킹기술의 특성상 경로를 파악할 수 없는 경우이다. (표 1)에서 알수 있듯이 국내 정보시스템들이 국외 해커에 의해 해킹 경유지로 이용되는 경우가 많다. 국내 시스템관리자들은 자신의 시스템이 해커에 공격을 받아 시스템 관리자 권한을 도용당했음에도 불구하고 이 사실조차 인지 못하는 경우가 많아 시스템관리자의 보안의식 및 지식이 시급히 요구되고 있다. 최근 국외의 유명한 보안관련 인터넷 사이트에서 한국 인터넷의 보안상태가 엉망이라는 질책들이 있었던 것도 명심하여야 한다.

그나마 다행인 것은 최근들어 국내에서의 해킹사고 신고가 늘어나고 있는데 이는 해킹에 대한 인식이 일반인들에게도 조금씩 늘어나고 있기 때문으로 분석된다. 국내에서 접수되는 해킹사고의 많은 부분은 개인 PC에 대한 윈도우즈 트로이목마 공격이다.

최근 윈도우즈 트로이목마는 바이러스와 함께 윈도우즈 시스템에 대한 새로운 위협으로 등장하였는데, 그 피해는 시스템 파괴, 응용프로그램 및 시스템 서비스 거부, 사용자 ID 및 패스워드 유출, 문서 유출 등 매우 다양하여 바이러스에 비해 훨씬 심각한 피해를 입히고 있다.

트로이목마는 정상적인 기능을 하는 프로그램으로 가장하여 프로그램 내에 숨어서 의도하지 않은 기능을 수행하는 프로그램의 코드 조각을 말한다.

최근 공격에 많이 사용되는 윈도우즈 트로이목마 프로그램들은 백오리피스(Back Orifice), 넷버스(NetBus), Sub7 등이 대표적이며, 이외에도 100여 가지 이상의 트로이목마 프로그램이 존재한다. 계속적인 기능 확장과 GUI의 편의성으로 인하여 윈도우즈 트로이목마 피해가 증가하고 있는 추세이다. 실제 국내에서 신고된 트로이목마 해킹사고의 공격자는 중·고등학교 학생들이 많았는데 이들은 해킹 시도가 법적인 처벌을 받는다는 사실을 인식못하고 호기심으로 저지르는 경우가 많았다. 또한 이들은 회사와 같이 고정된 IP주소를 가지고 있지 못하고 통신회사를 거쳐 동적으로 할당된 IP주소를 가지고서 공격을 하고 있으므로 추적이 쉽지 않고 통신회사에 보안전담 요원이 존재하는 경우가 많지 않기 때문에 호기심 많고 나이 어린 해킹 추종자들의 선부른 해킹 시도가 줄어들지 않고 있다.

호기심 차원의 해킹사고가 증가하는 것과 함께 전문 해커에 의한 악의적인 해킹 또한 크게 증가하고 있다. 일본 정부기관의 홈페이지 해킹사고, 야후 등 유명 인터넷 사이트에 대한 해킹사고 등은 이미 호기심 차원을 넘어서 특정 목적을 가진 의도적인 해킹이라고 할 수 있다. 이러한 경향의 해킹 성향을 핵티비즘(Hacktivism)이라고도 한다. 핵티비즘은 정부정책 비난, 난민들의 인권보호, 핵무기 사용과 원자력 발전소 건설 반대, 독재 정권에 대한 반발 등에 대한 정치/사회운동가 들의 호소내용이 주를 이루고, "적극적 행동주의"로 설명 될 수 있다[2].

다음은 행동주의자들에 의한 대표적인 해킹사례이다.

- UNICEF 해킹사고 (98. 1. 7)
  : 해커 Kevin Mitnick에 대한 석방을 요구
- 인도네시아 경찰청 사이트 해킹사고 (98. 1. 18)
  : 반 수하르토(Suharto) 대통령 시위의 일환으로 여당 사이트, ISP 등 공격.
- 미 육군 웹사이트 해킹사고 (98. 10. 28)
  : 핵무기 사용 반대
- 영국의 Time/Warner's Cartoon Network 웹사이트 해킹사고 (98. 10. 31)
  : 불가리아 어린이들에게 관심을 보내달라는 정치적 호소
- New York Times 웹사이트 해킹사고 (98. 9. 13)
  : 주요 언론기관에 대한 해킹으로는 최초의 사건으로 기자 및 Kevin Mitnick의 석방을 요구

국내의 경우 국가의 인터넷과 정보통신 기반은 급격한 증가를 보이고 있으며 금융, 통신, 공공기반시설 등 전 사회 분야가 인터넷 가상공간을 활용하기 시작하고 있다는 점을 감안할 때 이러한 사이버 테러 행위는 심각한 위협이 아닐 수 없다.

국내 해킹사고가 매년 큰 폭으로 증가하고 있고 대부분의 해킹이 국외 해커에 의해 발생되고 있다는 점을 감안하면 이러한 해킹으로 인해 국가 경제와 안보에 심각한 문제를 일으킬 수 있다.

그러면 왜 해킹이 이처럼 큰 폭으로 증가하고 있으며 국외 인터넷 보안 포럼에서 국내 보안 실태가 거론될 정도로 보안에 문제가 있는지 한번 고민해 봐야할 것이다.

첫째, 정보시스템의 활용도가 높아졌으며, 인터넷 등 네트워크를 통하여 서로 연결되어 있다. 최근 각 정보시스템들이 내부적으로는 LAN에 의해 연결되어 있고, 또한 인터넷에 연동되어 전세계의 어디든지 시간과 공간의 구애를 받지 않고 정보를 교환하고, 각종 서비스를 제공받을 수 있도록 되어 있다. 국내 인터넷 사용자 수가 이미 1천만명을 넘어 섰으며, 세계 10위권 내의 인터넷 강국으로 자리매김하고 있다. 반면에 네트워킹화에 따라 내부 사용자뿐 아니라 전세계의 어느 사용자라 할지라도 내부 시스템에 불법적으로 접근할 가능성이 높아졌다. 실제 국내 정보시스템 침해사고의 상당부분이 국외 해커에 의해 이루어졌다[3].

둘째, 해커들간의 자유로운 정보의 교환이다.

해커들은 자신들의 웹페이지를 만들어서 해킹기술을 인터넷에 자유로이 공개하고 있어 누구나 해킹 정보를 쉽게 구할 수 있다. 예전에는 인터넷을 이용하는 국내 몇몇 대학들의 전유물로 여겨지던 네트워크 침입 등의 해킹이, PC 통신과 인터넷이 연동되고 인터넷 상에서 쉽게 해킹도구를 구할 수 있으므로 컴퓨터에 대한 전문지식이 없는 이도 해킹할 수 있는 환경에 이르게 되었다.

셋째, 정보시스템 관리자의 시간적 · 기술적 역량 부족을 들 수 있다. 정보시스템을 공격하려고 하는 수많은 해커들은 공격 기술에 심취해서 정보시스템을 공격하려고 하고 있지만, 정보시스템의 관리자는 기관의 수많은 시스템을 관리하여야 하며, 고유 업무에 많은 시간을 빼앗겨 보안에 신경을 쓰기가 쉽지 않다. 최근에는 정보보호에 대한 인식이 많이 확산되어 관리자들이 정보보호를 위해 대처하려고 하지만 막상 정보보호에 대한 지식의 결여로 인해 실천에 옮기기는 쉽지 않은 실정이다.

이러한 이유들로 인하여 정보시스템에 대한 공격은 매년 증가하고 있어 전자상거래, 전자 정부 등 사이버 공간에서의 활동 증가에 따른 안전 신뢰성 해결이 위협받고 있다.

Ⅲ. 국내 해킹사례 및 해킹기술 분석

1. 유닉스 시스템 해킹사고

유닉스 시스템은 다수의 사용자가 이용할 수 있고

다양한 네트워크 서비스가 제공되고 있으며 운영체제가 공개되어 있어 해커들의 주요 목표가 되고 있다. 윈도우즈 시스템에 대한 트로이목마 공격이 나오기 전까지는 대부분의 공격이 유닉스 시스템에 집중되어 있었으며 현재에도 많은 부분의 해킹시도가 유닉스 시스템을 대상으로 하고 있다. 유닉스 시스템에 대한 해킹공격은 일반적으로 다음과 같은 순서를 거쳐 이루어지고 있다.

1. 네트워크 스캔을 통한 해킹 취약점 파악
2. 발견된 보안취약점 공격에 의한 계정 획득
3. 스니퍼 설치를 통한 네트워크 모니터링
4. 재침입을 위한 백도어 설치
5. 홈페이지 삭제, 자료유출, 타시스템 공격 등 불법행위
6. 침입흔적 인멸을 위한 로그 삭제

이러한 일반적인 불법침입 이외에도 원격지에서 시스템을 마비시키는 서비스거부 공격도 최근에 많이 이용되고 있다[6].

다음은 CERTCC-KR에 접수된 유닉스 시스템 해킹사례이다.

□ 사건 경위

'99년 11월 4일 영국의 대학망과 연구망의 보안을 담당하는 JANET-CERT로부터 국내의 K 대학에서 영국의 대학들을 상대로 보안취약점을 스캔하고 있다는 보고를 받았다. 공격을 시도하는 IP 주소를 추적한 결과 해당 시스템은 K 대학의 한 연구실에서 운영하는 리눅스 서버로 이 시스템 역시 에스파니아로부터 해킹을 당한 것으로 나타났다.

공격자는 K 대학의 시스템을 해킹한 후 영국, 캐나다, 대만, 미국 대학들, 미국 기업들 등 모두 186,547 사이트를 대상으로 해킹가능한 보안 취약점 정보를 수집하였다. 또한 보안취약점이 발견된 사이트에 대해서는 실제 해킹도구를 이용하여 해킹을 시도한 것으로 보인다.

□ 사건 분석 및 대응

이 사건은 국외에서 국내 시스템을 해킹한 후 다시 국외 기관을 공격하는 국내 시스템을 해킹 경유지로 이용한 전형적인 사례이다.

해당 시스템을 분석한 결과 공격자의 공격과정은 다음과 같았다.

① mountd를 이용한 시스템 침입

이 피해시스템은 mountd라는 프로그램의 버퍼 오버플로우 취약점을 이용하여 원격지에서 불법적으로 침입당하였다. mountd는 보안취약점이 널리 알려진 서비스로 이 취약점으로 인해 원격지에서 시스템 관리자 권한을 획득당할 수 있다. 아래는 /var/log/messages 로그파일에 남아 있는 mountd 공격 흔적이다.

```
Oct 27 06:01:00 xxx 28>Oct 27 06:01:00 mountd[288]: Blocked
attempt of 123.45.67.89 to mount
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^
P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^
P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^
P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^
P^P^P^P^
...
```

mountd는 최근 RPC(Remote Procedure Call) 서비스의 일종으로 rpc.statd, rpc.cmsd, rpc.ttdbserve 등과 함께 시스템의 해킹에 많이 이용되고 있다[7].

일반적으로 관리자들이 이들 서비스들이 불필요함에도 불구하고 서비스를 해주는 경우가 많은데 /etc/inetd.conf 에서 해당 서비스들을 중지시키거나 부팅시 자동으로 실행되지 않도록 RC 디렉토리를 수정하도록 한다. 또 반드시 필요한 서비스일 경우 각 운영체제 제조회사에서 제공되고 있는 보안패치 프로그램을 설치하여야만 한다.

② 해킹 프로그램 설치 및 운영

공격자는 침입 후 숨겨진 디렉토리(/dev/. /. /dev/ssddaa6699/. /)에 각종 해킹 프로그램들을 설치하고, 영국, 캐나다, 미국 대학들, 미국 기업들, 대만 등을 대상으로 해킹시도를 하였다. 공격자가 실제 공격에 앞서 가장 먼저 하는 행위가 해킹가능한 보안취약점을 찾는 것이다. 지난 '98년 6월에 발표된 mscan이라는 대규모 네트워크 스캔 도구와 함께 최근 여러 가지 취약점 스캔 도구들이 해킹에 사용되고 있다. 아래 파일들은 공격자가 설치한 공격 프로그램들과 국외 시스템의 보안취약점을 스캔한 결과물들이다.

README	cx.mountd	imapver*
robo8*	th	adm*
cx.named	imapvun*	rr.com
uk	automountd*	edu
kj/	rr.com.mountd	uk.mountd
autonamed*	edu.mountd	LPs*
..		

③ 네트워크 도청

공격자는 해킹한 시스템에 sniffer라는 네트워크 도청 도구를 설치하여 K 대학의 네트워크를 도청하였다. 한 시스템에 해킹 공격 후 네트워크 도청은 해커들의 일반적인 행위로 이를 통해 해킹한 시스템뿐만 아니라 다른 시스템의 사용자 ID와 패스워드까지도 알아낼 수 있다. 따라서, 해킹당한 시스템으로 인해 해당 기관의 네트워크 전체가 공격을 당할 수 있다. 해당 시스템이 sniffer 등에 의해 모니터링 당하고 있는지를 확인하기 위해서는 'ifconfig'라는 명령어를 사용하거나 ifstatus, CPM (Check Promicuous Mode)등의 공개 도구를 이용하여 점검할 수 있다.

④ 재침입을 위한 백도어 설치

최초 시스템을 공격하기 위해서 mountd 취약점을 이용하였지만, 차후에 쉽게 그리고 발견되지 않고 침입하기 위해서 백도어를 설치하였다.

해당 시스템의 login, in.telnetd 등을 변경하여 "rewt"라는 계정으로 들어올 경우 시스템관리자 권한을 부여하도록 하였으며, inetd 환경을 변경하여 6969번 포트로 접근할 경우 역시 시스템 관리자 권한의 쉘을 부여하도록 하였다.

이러한 백도어 설치도 역시 해커들의 일반적인 행위로 차후 재침입과 침입사실을 숨기기 위해 사용하고 있다. 백도어 설치를 위한 대표적인 해킹도구는 루트킷(Rootkit)으로 시스템의 각종 프로그램들을 트로이버전으로 변경하므로 루트킷 공격을 받으면 시스템을 다시 설치하여야만 한다.

2. 윈도우즈 시스템 해킹사고

윈도우즈 시스템의 해킹사고의 대부분인 트로이목마 피해사례는 꾸준히 보고되고 있는데 지난 '99년 한해동안 백오리피스(BackOrifice), 넷버스(NetBus) 등 윈도우즈 트로이목마 피해 및 해킹시도 신고가 모두 35건 접수되었다. 올해에도 유료 게임 프로그램의 ID 도용 등 트로이목마로 인한 해킹 신고가 계속 접수되고 있다. 하지만 이러한 사고의 공격자는 대부분 전화접속 사용자로 동적 IP 주소로 인한 추적의 난해함, 인터넷 서비스 제공업체(ISP) 등의 보안인력 부족, 공격자 연령층이 상대적으로 낮아 해킹의 불법성 인식부족 등 여러 가지 이유로 인해 해킹사고는 줄어들고 있지 않다.

다음은 CERTCC-KR에 접수되었거나 언론에 보도된 윈도우즈 트로이목마 관련 사례이다.

□ 사례 1

'99년 3월 서울 모대학교 L군은 과기대의 네트워크를 대상으로 개인 PC의 해킹프로램인 백오리피스가 설치되어 있는 시스템을 점검한 후, 백오리피스

를 이용하여 시스템 내 "우리별 3호"에 대한 정보 등 주요 정보를 탈취하였다. L군은 평소 해킹에 관심이 많은 학생으로 자신의 홈페이지에 해킹하는 방법 등 해킹 관련 자료들을 게시하였다. 또한 과기대로부터 탈취한 "우리별 3호" 등의 자료를 "자유 게시판"에 게시하기도 하였다. 이 사건은 피해기관 네트워크 담당자의 의뢰로 경찰청 컴퓨터 범죄 수사대에 신고되어 침입행위를 한 L군은 불구속 입건되었다.

□ 사례 2

'99년 11월 "에코키스"라는 윈도우즈 트로이목마를 이용하여 타인의 통장에서 현금을 인출해 간 20대가 경찰에 잡혔다. 취업을 위해 직업훈련원에서 컴퓨터 교육을 받은 22살 황 모씨는 에코키스를 받아 다른 사람의 PC통신 ID와 비밀번호를 알아 낼 수 있도록 변조하였다. 황씨는 해킹 프로그램을 E-mail로 위장해 PC 통신 가입자에게 보내는 수법을 썼다. 통신 가입자가 E-mail을 여는 순간 에코키스가 개인 PC에 설치되고 해킹이 시작된다. 이를 모르는 네티즌이 키보드를 조작하는 대로 해킹 프로그램에는 계좌번호와 비밀번호 등이 그대로 되었다. 이런 방법으로 황씨는 대전에 사는 한 모 씨의 PC뱅킹 계좌에서 140만 원을 계좌이체 시킨 후 현금으로 빼냈다 경찰에 꼬리를 잡혔다. 황씨가 도용한 ID는 250여개, 경찰은 또 다른 죄를 저질렀을 것으로 보고 있다.

□ 사례 3

2000년 1월 국내 머드 게임 사용자 Y씨는 자신의 게임 계정 및 패스워드를 도용당하였다. 게임계정을 도용한 공격자는 현금으로도 거래되고 있는 게임 아이템들을 자신의 계정으로 옮겨 버렸다. 게임 아이템은 게임 메니아들 사이에서 수만원에서 수백만원까지 현금으로 거래되고 있다.

□ 사례 4

2000년 2월 서울 C PC방에서는 국내 여러 ISP 주소로부터 백오리피스 공격을 계속적으로 받아와 PC방 고객들이 불만을 호소하였으며, 이 중 3대의 PC가 재부팅이 되지 않는 등 심각한 피해를 입었다.

윈도우즈 트로이목마 공격에 의한 피해의 궁극적인 책임은 개인 PC 사용자에 있다고 할 수 있다. 시스템 사용자가 점검하여야 할 트로이목마 보안대책은 다음과 같이 정리할 수 있다.

- ○ 트로이 목마 프로그램에 대한 사용자들의 인식
- ○ 통신망, 인터넷을 통한 파일 다운로드 주의
- ○ 출처가 불분명한 메일 첨부물 실행 주의
- ○ 정품 소프트웨어 사용
- ○ 최신 백신 소프트웨어 사용(실시간 감시기 사용)
- ○ ROMBIOS 패스워드, 스크린세이버 패스워드 등을 사용하여 PC의 물리적 보안 강화
- ○ 네트워크 모니터링을 통한 침입 감시 (netstat -a를 이용한 감시 포함)

Ⅳ. 결 론

올 2월 초, 미국에서 일어난 야후, 아마존, CNN 등 유명 전자상거래 웹사이트에 대한 해킹은 세계각국이 앞다투어 투자하고 있는 인터넷 디지털 경제에 얼마나 심각한 악영향을 줄 수 있는지 여실히 보여주는 사건으로 기록되고 있다. 이번 사고로 야후 웹사이트만 약 1억2천만 달러의 피해를 입힌 것으로 추정되고 있어 국가가 추구하는 지식정보사회는 해킹이나 바이러스 등의 공격으로 일순간에 무너질 수 있다는 교훈을 남긴 것이다. 국외의 해킹사례 뿐 아니라 국내 해킹실태도 위험수위를 넘어서고 있어 사이버 공간에 대한 법제도 정비, 정보보호기술개발, 정보보호 인력양성 등 다각적인 노력이 실천되어져야만 하겠다.

※ 참고문헌

[1] 임채호 외, '99 해킹바이러스 현황 및 대응, 한국정보보호센터, 1999

[2] 임채호 외, '98 해킹 현황 및 대응, 한국정보보호센터, 1998

[3] 정현철, 보안취약점 분류법 고찰 및 보안취약점 자동보완시스템 구현, 1999

[4] 김라경외, '99 정보화 역기능 실태조사, 한국정보보호센터, 1999

[5] 한국인터넷정보센터, http://www.nic.or.kr

[6] 분산 환경에서의 서비스거부 공격 분석보고서, http://www.certcc.or.kr/paper/tr1999/1999010/tr1999010.html

[7] RPC관련 보안 취약점 및 대책, http://www.certcc.or.kr/paper/tr1999/1999008/tr1999008.html

[8] 윈도우즈 트로이목마 피해현황 및 보안대책, http://www.certcc.or.kr/paper/incident_note/2000001/in2000001.html

[9] http://www.cert.org/stats/cert_stats.html

[10] http://www.ja.net/CERT/JANET-CERT/monthly_reports.html

[11] http://www.jpcert.or.jp/nl/

정 현 철

1996년 서울시립대학교 전산통계학과 졸업(이학사)
1999년 광운대학교 전산대학원 졸업(이학석사)
1996년~현재 한국정보보호센터 연구원
관심분야 : 시스템 및 네트워크 보안

임 채 호

1986년 홍익대학교 전자계산학과 졸업(학사)
1990년 건국대학교 전자계산학과 졸업(이학석사)
1995년 홍익대학교 전자계산학과 박사과정 수료
1985년~92년 KIST 시스템공학연구소 선임연구원
1992년~95년 대전실업전문대학 전자계산과 교수
1995년~96년 KIST 시스템공학연구소 선임연구원
1996년~현재 한국정보보호센터 선임연구원
관심분야 : 인터넷 보안, 분산시스템 보안