□특집□

분산서비스거부공격 등 최근 해킹기법과 대응방안

정현철† 조용상† 김상철† 이현우† 박정현†† 임채호††

◈ 목 차 ◈

1. 서 론

새천년은 해킹과 함께 시작되었다고 해도 과언은 아닐 것이다. 연도변환시기인 Y2K 기간 동안 컴퓨터의 연도인식 오류에 의한 혼란과 더불어 이 기간을 틈탄 해킹·바이러스 공격이 심각할 것으로 예상되었다. 다행히 이 기간에는 철저한 사전준비와 대응체제 구축으로 인해 큰 피해없이 무사히 넘기는 듯 했다. 하지만 얼마 지나지 않아서 일본 정부기관 홈페이지가 해킹당하고, 미국의 유명 인터넷 사이트들이 해킹으로 인해 마비되는 사태가 발생되었다. 이로 인해 각국에서는 인터넷 보안을 위한 예산을 증액한다, 보안인력을 양성한다, 법·제도를 정비한다는 등의 대책을 하나하나 내놓고 있다. 국내에서도 이러한 해킹사고는 매년 큰 폭으로 증가하고 있어 이에 대한 대비가 절실한 실정이다.

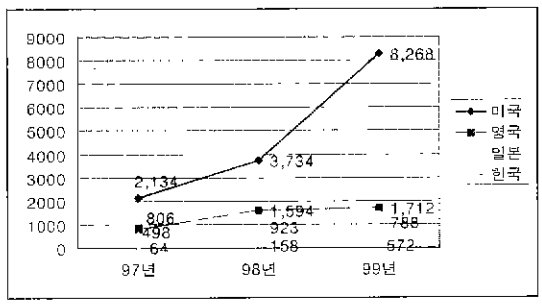
본 고의 제 2장에서는 지난 '99년 한해동안 국내에서 발생된 해킹사고 현황을 소개하도록 하고 제 3장에서는 야후, CNN, 아마존 등 세계 주요 인터넷 사이트의 공격에 사용된 분산서비스거부 공격에 대하여 살펴보도록 하고, 제 4장에서는 분산서비스거부공격 이외에 최근 시스템 해킹에 사용되고 있는 해킹기법과 그 대응방안에 대해 알아보고, 제 5장에서 결론을 내리도록 한다.

† 정회원 : 한국정보보호센터 연구원
†† 정회원 : 한국정보보호센터 선임연구원

2. 1999년 국내·외 해킹사고 분석

2.1 해킹사고 현황

'99년은 '98년의 156건에 비하여 3배 이상 늘어난 572건의 해킹사고가 보고되었다. 이러한 현상은 미국, 영국, 일본도 마찬가지로 전세계적으로 해킹사고는 크게 증가하고 있다는 것을 알수 있다[1, 8, 9, 10].



(그림 1) 국외 해킹사고 증가 추이

<표 1>은 '99년 초반기에 약 2~30건의 해킹사고가 접수되었으며 중반기에 약 40여건의 해킹사고가 접수되었고, 연말경에는 약 100여건으로 해킹사고가 급속히 증가하였음을 보여주고 있다.

〈표 1〉 기관별 해킹 피해 건수

월	대학 (ac.kr)	기업 (co.kr)	비영리 (or.kr)	연구소 (re.kr)	기타 (지역 등)	계
1월	15	12	0	0	0	27
2월	23	8	1	0	2	34
3월	17	8	0	0	1	26
4월	16	16	1	0	1	34
5월	11	18	2	0	1	32
6월	17	20	0	1	2	40
7월	20	22	2	1	0	45
8월	10	18	9	0	6	43
9월	16	19	2	1	0	38
10월	20	20	0	0	1	41
11월	67	33	5	7	4	116
12월	30	54	0	1	11	96
합계	262	248	22	11	29	572

기관별 해킹 피해 접수현황을 살펴보면 대학이 262건(45.8%)로 가장 많은 해킹사고가 접수되었으며 일반기업이 248건(43.4%)로 두 번째로 많은 사고가 접수되었고, 지역 등의 기타가 29건(5.1%), 비영리기관이 22건(3.8%), 연구소가 11건(1.9%) 순으로 접수되었다. 12월에 지역 도메인에 대한 해킹사고가 다수 접수되었는데 이들은 대부분 초·중등학교의 리눅스 서버로 방학기간동안 시스템 관리자의 관리소홀로 인해 지속적으로 공격을 당하였다.

국내·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 2> 국내 국제간의 피해관계

	국내-> 국내	국내-> 국외	국외 -> 국내		N/A	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 피해기관에서 자체적으로 분석한 경우로써 이들 중에서도 많은 부분이 국외에서 침입한 것으로 보고 있다. <표 2>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.

국내 해커에 의한 공격은 72건(12.1%) 발생하였으며 이들은 대부분 백오리피스 등 윈도우즈 시스템에 대한 공격이었다.

2.2 해킹기법 분석

해킹발생건수의 증가와 함께 해킹기법도 점점 지능화, 고도화 되어가고 있는데 바이러스와 마찬가지로 자기복제 능력을 가진 밀레니엄 인터넷 웜(Millennium Internet Worm)이 국내 피해시스템에서 발견되기도 하였으며 대규모의 해킹피해시스템을 이용하여 특정 시스템을 공격하는 분산서비스 거부 공격도구가 발견되기도 하였다.

지난 '98년에 개발된 대규모 스캔공격 도구인 mscan 이후 수많은 스캔도구들이 개발되어 해킹에 사용되고 있다. 인터넷 상에 운영되고 있는 시스템이라면 누군가 보안취약점을 훔쳐보고 있다는 사실을 명심하여야 한다.

'99년 한해 동안 시스템에 불법적인 침입은 대부분 버퍼오버플로우 버그로 인해 발생되었다. 특히, 버그가 알려진 RPC 서비스들이 주요 공격의 목표가 되었다. 리눅스 레드햇 5.x 버전의 경우 mountd에 의해 많은 공격을 당하였고, 레드햇 6.x

버전의 경우 amd 취약점에 의해 많은 공격을 당하였다. 또, '98년과는 달리 리눅스 서버뿐만 아니라 중형 시스템인 솔라리스 시스템도 피해 접수가 많이 되었다. 솔라리스 시스템의 해킹에 사용된 기술은 rpc.cmsd, ttdbserverd, rpc.statd, automountd, rpc.sadmind 등이었다[3].

다음 <표 3>은 '99년 해킹사고에 사용된 해킹 기법이다.

〈표 3〉 해킹에 사용된 공격 기법

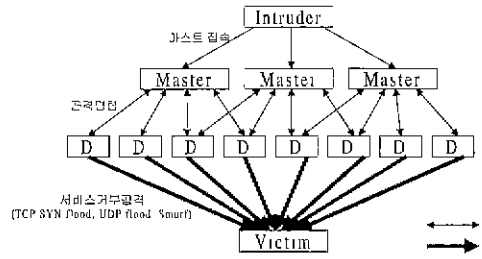
분 류	공격 방법	횟수	분 류	공격 방법	횟수
서비스거부 공격 (16)	smurf	9	사용자 도용 (68)	sniffer	38
	ping flooding	1		brute force	4
	SYN flooding	1		crack	6
	nuke	1		디폴트 계정 도용	2
	Trinoo	3		기타	18
	기타	1	S/W 보안오류 이용(3)	phf-CGI 등	3
E-mai 관련 공격 (20)	spam mail	19	버퍼오버 플로우 취약점 (214)	popd	19
	mail bomb	1		imapd	22
취약점 정보수집 (272)	mscan	41		mountd	45
	sscan	5		named	16
	imapd scan (143 port)	21		amd	23
	popd scan (110 port)	9		ftpd	32
	named scan (53 port)	3		rpc.statd & automountd	20
	ftpd scan (21 port)	24		rpc.ttdbserver	2
	CGI scan (80 port)	1		rpc.cmsd	6
	SUN RPC scan (111 port)	60		ufsrestore	1
	백오리피스 scan	5		기타	28
	Net Bus scan	4	구성·설정 오류 (2)	신뢰관계 이용	1
	port scan	89		기타	1
	기타	10	악성 프로그램 (58)	Back Orifice	25
사회공학(4)	패스워드노출 등	4		NetBus	1
				rootkit	27
				백도어	3
				인터넷웜	1
				기타	1

3. 분산서비스거부공격의 이해 및 대응방안

3.1 분산서비스거부공격 개념 및 사례

2000년 2월 7일 세계적 인터넷 사이트인 Yahoo가 해킹공격을 당한 후 연이어 EBay, Amazone, CNN 등 주요 사이트들이 공격을 받았다. 이들 사이트들은 50여개 이상의 다수의 시스템으로부터 초당 수백메가에서 수 기가에 이러는 엄청난 데이터를 받음으로써 수시간 동안 시스템이 마비되거나 서비스가 지연되었다. 이들 국외 유명사이트의 공격에 사용되었던 해킹기술이 바로 분산서비스거부공격(Distributed Denial of Service Attack)이다.

분산 서비스 거부 공격이라 함은 많은 수의 호스트들에 패킷을 범람시킬수 있는 DoS공격용 프로그램들이 분산 설치되어 이들이 서로 통합된 형태로 어느 목표 시스템(네트웍)에 대하여 일제히 데이터 패킷을 범람시켜서 그 표적 시스템(네트웍)의 성능저하 및 시스템 마비를 일으키는 기법을 말한다[2, 4, 5, 6]. 다음은 분산서비스거부 공격 개요도이다.



(그림 2) 분산서비스거부 공격 개요도

이러한 DoS공격은 TCP SYN flooding공격, UDP flooding공격, ICMP echo requesting공격, ICMP broadcasting 공격(Smurf공격) 등의 형태로 나타나며, 이러한 공격을 수행하기 위해서 다양한 tool이 제작되었다. 그중 최근에 문제가 되는 것은 최근 (2000년 2월) 미국 yahoo 등의 주요 인터넷 사

이트를 수 시간 동안 작동불능 상태로 빠뜨린 사건으로서, TFN2000 (TFN2K) 과 Stacheldraht 등 신종 분산서비스거부 공격도구가 사용되었다.

국내에서도 이미 '99년 8월 10일 분산서비스거부공격 도구의 하나인 trinoo에 의한 공격이 처음으로 발견되었으며 이후의 침해사고 처리과정에서 대규모적으로 발견되고 있다. 국내 Y 대학의 경우 50여 호스트에 trinoo 마스터 및 데몬이 설치되어 있었으며 이들로 인해 Y 대학 네트워크 속도가 현저히 저하되었던 사건이 발생했었다. 또, 2000년 2월 네트워크 속도가 현저히 떨어져 CERTCC-KR에 해킹분석을 의뢰했던 인터넷 회사의 경우 국외 유명 인터넷 사이트를 공격하는데 사용되었던 TFN2K가 설치되어 있었다. 국내도 이러한 분산서비스거부 공격의 안전지대는 아니며 언제든 외국해커들의 목표물이 될 수 있다.

3.2 분산서비스거부공격 대응방안

분산서비스거부공격을 받게되면 다양한 IP 주소에서 다양한 포트로 엄청난 양의 데이터가 쏟아져 들어오므로 확실한 해결책은 존재하지 않는다. 공격지 주소 또한 위장되어서 들어올 수 있으므로 더더군다나 대응이 힘들어 진다. 또 이러한 공격 도구들은 일반적으로 해킹당한 시스템에 설치되어 공격을 하기 때문에 모든 기관이 서로 보안에 신경을 써야만 한다.

하지만 다음과 같은 기본적인 해결책을 생각해 볼 수 있다.

첫째, 자신의 시스템에 분산서비스거부 공격 도구가 설치되지 않도록 한다.

자신의 시스템에 분산서비스거부 공격 도구가 설치되어 공격에 이용당하지 않게 하기 위해서는 시스템을 항상 안전하게 유지하여야만 한다. 이러한 도구가 설치된 대부분의 시스템들은 보안이 허술하여 공격받고 있는데, 운영체제나 응용프로그램의 주기적인 패치를 비롯한 기본적인 보안관리에 신경을 써야만 한다. 특히, Linux 시스템의 amd 유틸리티, mountd 데몬, 그리고 솔라리스 시스템의 RPC 서비스 취약점으로 인해 많은 공격을 받고 있으므로 이들에 대한 패치에 주의하여야만 한다.

둘째, 자신의 네트워크에서 소스 IP주소가 위장되어서 나가는 패킷을 막는다. 대부분의 서비스거부공격은 소스 IP를 위장하여 공격하므로 라우터나 침입차단시스템에서 위장된 주소를 가진 패킷을 차단한다.

셋째, 분산서비스거부공격을 신속히 탐지한다.

각 기관에서 사용되고 있는 침입탐지시스템(IDS)들은 최근 큰 문제가 되고 있는 분산서비스거부공격을 탐지할 수 있는 기능을 가지고 있다. 또, 네트워크 스캔 도구나 모니터링 도구를 이용하여 자신의 네트워크 내에 공격 데몬이나 마스터가 깔려져 있는지 탐지할 수 있다.

다음은 각 분산서비스거부 공격 도구이 사용하는 포트나 프로토콜들이다.

〈표 4〉 DDOS 공격도구별 특징

DDOS 공격 도구	특 징
trinoo	1524 tcp, 27665 tcp, 27444 tcp, 31335 udp 사용
TFN	ICMP ECHO, ICMP ECHO REPLY 사용
Stacheldraht	16660 tcp, 65000 tcp, ICMP ECHO, ICMP ECHO REPLY 사용
TFN2K	통신에 특정 포트가 사용되지는 않고 UDP, ICMP, TCP 등이 복합적으로 사용된다. 아마도 실행시에 포트번호가 정해지거나 프로그램에 의해 임의의 포트가 선택되어 지는 듯 함

미국의 국가 기반구조 보호센터(National Infrastructure Protection Center)에서는 이러한 DDOS 공격 도구를 탐지할 수 있는 툴을 제공하기도 한다[11].

넷째, 만일 분산서비스거부공격 도구가 발견되

면 신속히 보고한다. 발견된 공격도구에는 분산공격에 이용당하고 있는 다른 시스템들에 대한 정보도 포함되어 있을 수 있으므로 이들기관과 CERTCC-KR에 신속하게 보고하도록 한다.

다섯째, DDOS 공격을 받을 경우 네트워크 차원에서의 접근통제한다.

대규모 데이터를 보내는 공격 주소로부터의 모든 패킷을 차단한다. DDOS 공격의 특성상 공격자 주소는 하나가 아닌 수십개가 될 수도 있으며 위장된 주소일 가능성도 있다. 또, 단위시간 동안 일정량 이상의 SYN 패킷이나 ICMP 패킷이 들어올 경우 이를 차단할 수 있도록 라우터나 침입차단시스템을 설정한다.

분산서비스거부 공격은 여러 사이트가 연계된 사고이므로 관련 사고가 발생하게 되면 신속히 CERTCC-KR에 신고하여 공동으로 대응할 수 있도록 한다.

4. 기타 해킹기법 및 대응방안

3장에서 살펴본 분산서비스거부공격은 이미 해킹을 당한 여러 시스템에 서비스거부공격 도구가 설치됨으로써 가능하다. 즉, 분산서비스거부공격도 시스템이 침해당한 결과로써 나타나는 피해현상이다. 그러면 최근에 시스템이 침해당하는 것은 어떠한 해킹수법에 의한 것일까. 그것은 버퍼오버플로우(Buffer Overflow) 공격이다. 버퍼오버플로우 공격은 프로그램내에서 지정된 버퍼크기보다 더 많은 양의 데이터를 버퍼에 입력하여 다른 영역까지 영향을 미치게 만드는 공격방법이다. 그 결과로 원격지에서 시스템관리자 권한을 획득할 수 있다. 최근 CERTCC-KR에 보고된 해킹사고는 <표 3>에서 보이는 것처럼 이러한 버퍼오버플로우 공격에 의해 발생되고 있는데 가장 대표적인 것이 rpc.statd, automountd, ttdbserverd, rpc.cmsd 등 Solaris rpc 관련 취약점과 Linux의 amd, mountd 취약점 등에 대한 공격이다[3].

유닉스 시스템에 대한 공격으로 버퍼오버플로우 공격이 대표적이라고 하면 윈도우즈 시스템에 대한 공격은 트로이목마 공격이 대표적이다.

본 장에서는 유닉스 시스템의 버퍼오버플로우 공격과 윈도우즈 트로이목마 공격에 대하여 살펴보고 그 대응방안에 대해서 알아보도록 한다.

4.1 유닉스 버퍼오버플로우 공격 및 대응

4.1.1 rpc.statd

rpc.statd는 시스템 장애시 NFS에서의 파일 복구를 위해 제공하는 lockd를 지원하며 클라이언트와 서버의 상태를 모니터링하는 rpc프로그램이다. 하지만 원격 클라이언트의 매개변수 크기를 체크하지 않기 때문에, 스택오버플로우를 통해 루트권한에서만 수행 가능한 임의의 명령어를 수행시킬 수 있다[12,14].

4.1.2 automountd

솔라리스 시스템의 automountd는 일반적으로 UDP나 TCP프로토콜을 통해서는 패킷을 받아들일 수 없지만 rpc.statd가 포워딩해 주는 TLI프로토콜을 통해서는 패킷을 받아들일 수 있다. 공격자는 이를 이용해 자신이 실행시키고자 하는 명령어를 rpc.statd에 패킷으로 보내 실행시킬 수 있다. 공격자는 원격 시스템에서 공격 대상 시스템의 rpc서비스 정보를 살펴보고 rstatd데몬이 실행되고 있는지 확인할 수 있다[14].

다음은 rstatd 데몬이 실행되고 있을 경우 automountd 취약점 공격 프로그램을 이용하여 특정 명령어를 실행시켜 루트로 접속하는 예이다.

```
# amountdexp abc.victim.com victim "echo + + >    /.rhosts" 0
 SM_MON  0
 SM_NOTIFY· 0
# rsh abc.victim.com -l root csh
 id
 uid=0(root) gid=1(other)
```

4.1.3 rpc.ttdbserved

ttdbserver는 RPC기반의 ToolTalk 데이터베이스 서버 프로그램인데, 이 프로그램의 구현상의 오류로 인해 원격의 침입자가 루트 권한으로 특정 명령어를 실행시킬 수 있다[15]. 이 취약점은 SUN 솔라리스뿐만 아니라 HP, IRIX, AIX등 대부분의 시스템에서도 나타난다.

4.1.4 rpc.cmsd

rpc.cmsd프로그램은 데이터베이스 관리 프로그램으로 Open Windows의 Calendar Manager와 CDE의 Calendar가 이용한다. 침입자는 이 프로그램의 취약점을 이용해서 원격에서 임의의 파일을 쓰거나 루트 권한을 얻을 수 있다[16]. 다음은 rpc.cmsd 취약점을 이용하여 관리자 권한을 획득하는 프로그램을 수행시킨 결과이다.

```
attacker# cmsdscan xxx.xxx.xxx.xxx
---[vetesgirl@iname.com]----

[Vetes cmsd scanner]: looking for c
[Vetes cmsd scanner]: checking for all the bitches arguments.
 right on
[Vetes cmsd scanner]: checking for CMSD vulnerability..
 right on
[Vetes cmsd scanner]: Seeing if we get in using Solaris 2.6 (1) .
right on
[Vetes cmsd scanner]  Seeing if we get in Solaris 2.5.1..(2)
right on
[Vetes cmsd scanner]: Seeing if we get in using Solaris 2.5.1...(3)
right on
[Vetes cmsd scanner]: Seeing if we get in using Solaris 2.5 (4)..
right on
[Vetes cmsd scanner]· Seeing if we got root  .
right on

attacker# telnet xxx.xxx.xxx.xxx 1524
Trying xxx.xxx.xxx xxx...
Connected to xxx.xxx xxx.xxx.
Escape character is '^]'.
# id;
uid=0(root) gid=1(other)
```

4.1.5 Linux amd 공격 및 공격 탐지

RedHat Linux am-utils 패키지의 일부인 amd 데몬은 automountd와 유사한 프로그램으로 파일시스템을 마운트하는데 사용된다. 하지만 amd 데몬의 로깅기능에 버퍼오버플로우 취약점으로 인하여 원격에서 관리자 권한을 획득할 수 있다[17]. /var/log/messages 파일에 다음과 같은 로그를 확인함으로서 공격여부를 확인할 수 있다.

```
Jan  9 16:56·12 corona 27>Jan  9 16 56:12 amd[554]· amq
requested mount of
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?^~M^^P
~I^^~C?H~I^^D~C?C~I^^H~C?K~M^N
~I??IF^L~HF^W~HF^Z?K?@腕 8 Jan 1998--str/bin/sh(-c)/bin/
echo '2222
stream  tcp    nowait  root    /bin/sh s
```

자동화된 amd 공격도구에 의해 공격을 받았을 경우 /tmp/h 파일이 생성되고 2222번 포트를 통해 시스템관리자 권한의 쉘을 획득당할 수 있다.

4.1.6 유닉스 버퍼오버플로우 공격 대응방안

유닉스 시스템의 해킹에서 가장 일반적인 방법인 버퍼오버플로우 공격에 대비하기 위하여 관리자가 고려해야할 대응방안은 다음과 같다.

첫째, 보안패치를 적용한다.

버퍼오버플로우 공격은 시스템 운영체제나 응

〈표 5〉 운영체제별 보안패치 사이트

운영체제	패치 정보제공 사이트
SunOS/ Solaris	http://sunsolve.Sun com/sunsolve/us/pubpatches/patches.html ftp://sunsolve.sun.com/pub/patches/
AIX	http://aix.software.ibm.com/aix.us/swfixes/ ftp://aix.software.ibm com/aix/efixes/security/
HP-UX	ftp://us-ffs.external.hp.com/
IRIX	ftp://sgigate.sgi.com/security/
Linux	ftp://updates.redhat.com/
SCO	http://www sco.com/security/
Digital	http://www.service.digital.com/patches/index.html

용프로그램 내의 일종의 소프트웨어 버그에 대한 공격이다. 따라서 버퍼오버플로우 공격을 방지할 수 있는 가장 기본적인 방법은 각 시스템 회사에서 배포하는 보안패치를 적용하는 것이다. 다음은 각 운영체제별로 패치를 제공해 주는 사이트이다.

둘째, 불필요한 프로그램을 정지시킨다.

해커들의 공격대상이 되고 있는 버퍼오버플로우 취약점을 가진 네트워크 서비스들은 대부분 실제 사용되지 않는 서비스들이 많다. 그러므로 이러한 서비스들은 부팅시에 자동으로 실행되지 않게 하거나 /etc/inetd.conf에서 해당 서비스의 실행을 중지시켜야만 한다.

셋째, 버퍼오버플로우 차단프로그램 설치 운영한다. 만약 패치가 신속히 제공되지 않을 때 차단프로그램(Wrapper)으로 버퍼오버플로우를 해결한다.

4.2 윈도우즈 트로이목마 공격 및 대응방안

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 버해 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.

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.

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

5. 결 론

정보시스템들이 급속히 증가하고 인터넷을 통하여 서로 연결됨으로써 이미 전세계는 하나의 네트워크나 마찬가지이다. 인터넷이라는 거대한 단일망에서 국적은 의미가 없어졌으며, 해킹사고도 국적을 가리지 않고 발생되고 있다. 국내 해킹사고도 매년 3배 이상 크게 증가하고 있으며 이들 대부분이 국외 해커에 의한 소행이다. 하지만 국내에는 아직 자기 시스템을 스스로 보호할 수 있을 만큼의 실력을 가진 전문가가 많지 않고, 보안에 대한 투자 또한 극히 인색한 실정이다. 국내 정보화는 국외에서도 놀랄 정도로 훌륭하게 건설되어 가고 있는 반면 이를 관리하고, 안전하게 유지하기 위한 노력은 극히 부족하다. 외관상의 정보화 뿐만 아니라 진정 건전한 정보화 사회를 이끌어가기 위해서는 정보보호는 필수적이라 할 수 있다.

본 고에서는 최근 국내·외에서 발생된 해킹현황을 소개하였으며, 특히 최근 국외 유명사이트들의 공격에 사용되었던 분산서비스거부 공격에 대

하여 살펴보았다. 분산서비스거부공격은 DoS 공격용 해킹도구를 많은 시스템에 설치한 후 일시에 공격대상 시스템에 패킷을 범람시킴으로써 공격대상 시스템과 네트워크를 마비시켜 버리는 공격이다. DoS 공격용 해킹도구가 설치되는 시스템은 대부분 보안이 허술하여 이미 시스템관리자 권한을 빼앗겨 버린 시스템들이 많다. 시스템관리자 권한의 불법적인 획득을 위해서는 RPC 관련 버퍼오버플로우 취약점이 많이 이용되고 있다. 일반적인 해커들의 해킹과정을 살펴보면 실제 공격에 앞서 RPC 취약점 등을 가진 보안이 허술한 시스템을 찾기 위해 스캔공격을 수행한다. 한국정보보호센터에서는 해커들의 스캔공격을 자동으로 탐지할 수 있는 RTSD(Real Time Scan Detecter)를 홈페이지를 통하여 무상으로 보급하고 있으므로 이를 이용하여 해킹시도를 탐지하는 것도 좋은 대응방안이라고 생각된다.

유닉스 시스템에 대한 해킹뿐만 아니라 개인 PC에 대한 해킹사고도 빈번히 발생되고 있어 개인정보가 침해당하고 있다. 최근의 해킹수법들이 점점 전문화, 지능화되어 가고 있는 추세이므로 여기에 대응하기 위해서는 해킹대응 인력의 양성, 정보보호 예산의 증액, 법·제도 정비 등 다각적인 노력이 따라야만 한다.

참고문헌

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

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

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

[4] Distributed Denial of Service Tools, http://www.cert.org/incident_notes/IN-99-07.html

[5] Results of the Distributed-Systems Intruder Tools Workshop, http://www.cert.org/reports/dsit_workshop.pdf

[6] Analysis of trin00, BUGTRAQ@SECURITYFOCUS.COM

[7] Denial of Service Attack using the trin00 and Tribe Flood, ISS Security Alert

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

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

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

[11] http://www.fbi.gov/nipc/trinoo.htm

[12] http://www.cert.org/advisories/CA-97.26.statd.html

[13] http://www.cert.org/advisories/CA-98.12.mountd.html

[14] http://www.cert.org/advisories/CA-99-05-statd-automountd.html

[15] http://www.cert.org/advisories/CA-98.11.tooltalk.html

[16] http://www.cert.org/advisories/CA-99-08-cmsd.html

[17] http://www.cert.org/advisories/CA-99-12-amd.html

정 현 철

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

조 용 상

1998년 한국과학기술원 경영과학과 졸업(공학사)
1999년-현재 한국정보보호센터 연구원
관심분야 : Secure 네트워크 설계

김 상 철

1994년 아주대학교 산업공학과 졸업(공학사)
1996년 아주대학교 산업공학과 대학원 졸업(공학석사)
1995년-1999년 진양공업(계장)
1999년-1999년 Ako-Tech(과장)
1999년-현재 한국정보보호센터 연구원
관심분야 : 네트워크 보안관리

박 정 현

1988년 경북대학교 통계학과 졸업 (이학사)
1994년 LG 전자 시스템연구팀 주임연구원
1996년 한국물류정보통신(주) 시스템팀 과장
1996년-현재 한국정보보호센터 선임연구원
관심분야 : 시스템 및 네트워크 보안

이 현 우

1996년 숭실대학교 전자계산학과 졸업(공학사)
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