와레즈(컨텐츠 불법유통 사이트)등으로 악용되는 윈도우즈 해킹피해 대책

(Ver. 1.0)

CERTCC-KR

2004.01.20(수)

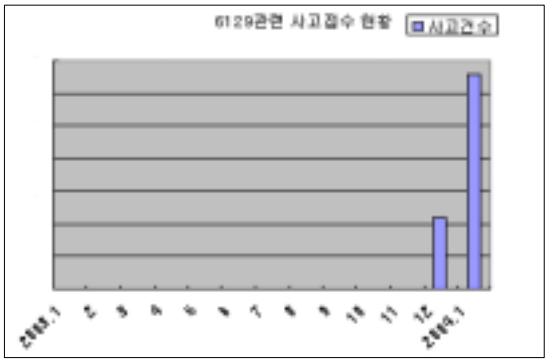
차명석 (mscha@kisa.or.kr)
김경희 (khkim@kisa.or.kr)

- 차 례 -

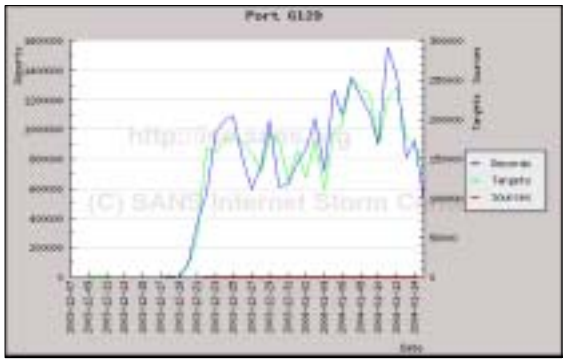
1. 개요
2. 해킹도구(DameWare, Radmin, Nethief)의 이해
3. 침해경로의 이해
4. 해킹피해 여부 판단방법
5. 피해복구 방법
6. 예방방법
7. 참고사이트

1. 개요

2003년 11월부터 한 두건씩 접수되던 TCP 6129 관련 스캔신고가 2004년 1월에 들어와 급격히 증가하였다. 아래의 (그림 1-1)에 보듯이 12월, 1월에 들어와 급격히 증가함에 따라 KRCERT에서는 원인분석 및 사례조사를 시작하였다. 또한 미국 incidents.org(그림 1-2)에서 보듯이 2003년 12월 19일 이후부터 TCP 6129 포트가 급격히 증가하고 있음을 보여주고 있다. (TCP 6129는 윈도우즈용 원격 관리도구인 DameWare Mini Remote Control의 설치시 기본으로 잡히는 서비스 포트이다)



(그림 1-1) 6129관련 신고접수 현황



(그림 1-2) TCP 6129 트래픽 추이

여기에서는 TCP 6129 침해사고 관련 피해시스템들을 분석하는 과정에서 밝혀진 침해경로에 대해서 설명하고, 침해사고를 여부를 판별하는 침해사실 탐지방법과 예방 및 대처방안에 대해서 제시하고자 한다.

본 문서는 인터넷 환경의 개선과 함께, 개인 사용자들의 시스템을 보호할 목적으로 만들어졌으며, 국내에 이미 알려진 사례를 통하여 작성되었다. 일부는 KRCERT에서의 자체 분석 결과를 토대로 작성되었다. 본 문서에서 언급한 내용 이외에도 수많은 공격기법과 취약점이 있지만, 일반 사용자 및 시스템 관리자가 꼭 알아두어야 할 내용과 대응방법에 대해서 언급하였다. 본 문서에서 다루어지지 않은 취약점 및 공격기법에 대해서는 KRCERT 홈페이지[1]의 보안권고문을 참조하길 바란다.

2. 해킹도구(DameWare, Radmin, Nethief)의 이해

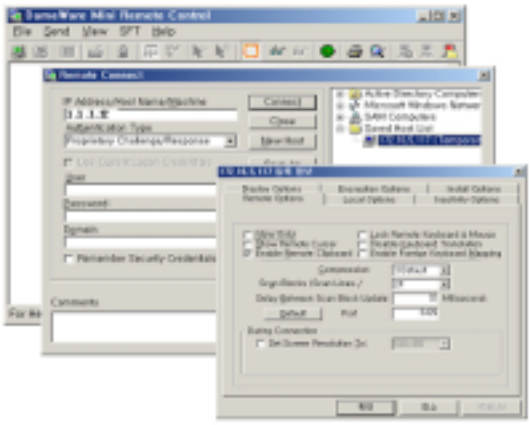
윈도우즈 관련 침해사고에서 Netbus와 Subseven이 백도어로 많이 사용되고 있다. 하지만 근래 DameWare, Radmin 그리고 Nethief을 이용하는 사고접수가 증가하고 있다. 기존에 잘 알려진 Netbus와 Subseven은 컴퓨터바이러스 백신을 이용해서 검사할 수 있지만, DameWare, Radmin, Nethief는 대부분의 백신에서 검출하지 않는 실정이다. 따라서 사용

1) http://www.certcc.or.kr

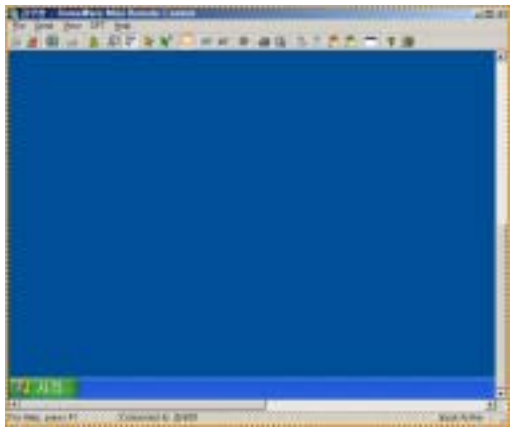
자가 해당 프로그램에 대한 이해를 하고, 점검방법에 따라서 정기적으로 점검하는 것이 중요하다.

1) DameWare Mini Remote Control

Dameware Mini Remote Control은 원격에서 Windows 95/98/ME/NT/2000/XP을 관리할 수 있는 도구로써 클라이언트/서버 구조로 되어 있으며, 원격제어 서버역할을 수행하는 DWRCS.exe(DameWare Remote Control Server)가 TCP 6129를 이용하여 서비스하도록 초기 설정되어 있다. 해당 실행파일은 윈도우즈 시스템폴더에 설치되며, 시스템이 시동될 때 함께 시작되도록 윈도우즈 서비스에 등록된다.



(그림 1-3) DameWare 클라이언트



(그림 1-4) DameWare 원격제어

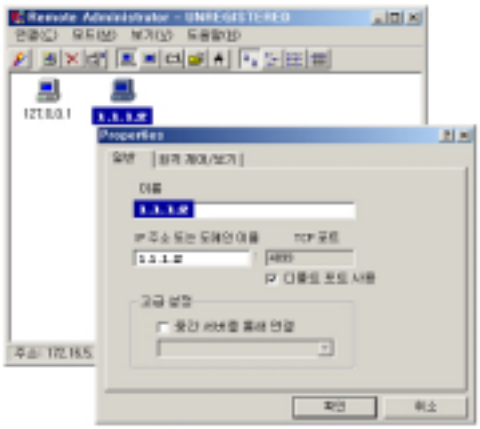
위의 (그림 1-3)은 DameWare 클라이언트에서 서버로 연결하기 위해서 설정하는 GUI로서 연결 포트번호와 인증방법 등을 설정할 수 있다. (그림 1-4)는 DameWare 클라이언트에서 서버로 연결한 GUI를 보여주고 있으며, 원격의 컴퓨터의 전체화면을 볼 수 있으며, 마우스나 키보드의 원격의 컴퓨터로 전달되어 마치 자기 앞에 있는 것처럼 제어할 수 있다.

DameWare Mini Remote Control 3.72와 그 이전 버전에는 Buffer Overflow취약점이 존재한다. 원격에서 조작된 Packet을 보내어서 DWRCS.exe 프로그램에서 사용하는 strcpy 함수에서 Buffer Overflow를 발생시킬 수 있으며, 윈도우에서 명령을 실행할 수 있는 쉘을 획득하여 임의의 코드를 실행할 수 있다. 따라서 DameWare Mini Remote Control를 사용하는 정상고객인 경우 최신버전으로 업그레이드해야 한다.

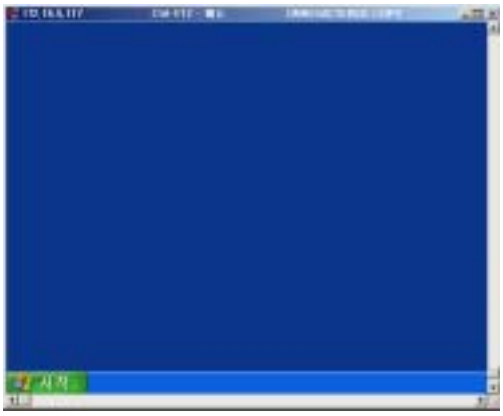
※참고 : DameWare는 'http://www.dameware.com/' 사이트에서 제공되며, 최신버전은 4.0이다.

2) Radmin

Radmin(Remote Administrator)은 DameWare와 같이 원격에서 Windows 95/98/ME/NT/2000/XP을 관리할 수 있는 도구로써 클라이언트/서버 구조로 되어 있으며, 원격제어 서버역할을 수행하는 r_admin.exe가 TCP 4899를 이용하여 서비스하도록 초기 설정되어 있다. 해당 실행파일은 윈도우즈 시스템폴더에 설치되며, 시스템이 시동될 때 함께 시작되도록 윈도우즈 서비스에 등록된다.



(그림 1-5) DameWare 클라이언트



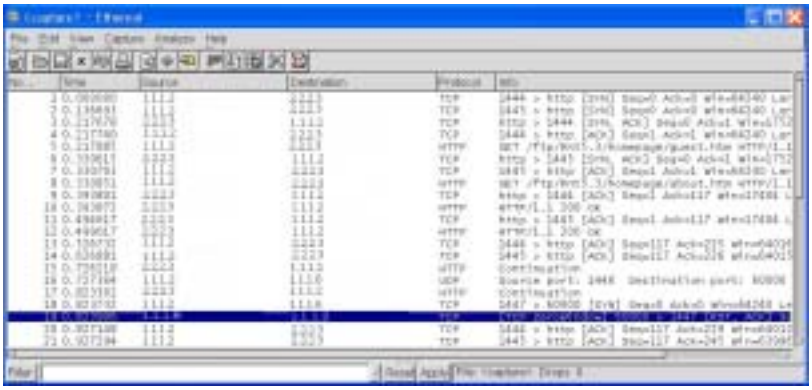
(그림 1-6) DameWare 원격제어

위의 (그림 1-5)는 Radmin 클라이언트에서 서버로 연결하기 위해서 설정하는 GUI로서 연결 IP주소와 포트번호 등을 설정할 수 있다. (그림 1-6)은 Radmin 클라이언트에서 서버로 연결한 GUI를 보여주고 있으며, DameWare와 마찬가지로 원격의 컴퓨터의 전체화면을 볼 수 있으며, 마우스나 키보드의 원격의 컴퓨터로 전달되어 마치 자기 앞에 있는 것처럼 제어할 수 있다. 초기 설정으로 Radmin 서버를 설치하는 경우, 패스워드가 Null로 설정된다. 따라서 관리목적으로 Radmin을 사용하는 경우 서버설치 시 패스워드를 반드시 설정해야 한다.

※참고 : Radmin은 'http://www.radmin.co.kr' 사이트에서 제공되며, 최신버전은 2.1이다.

2) Nethief

Nethief는 위의 DameWare와 Radmin처럼 원격관리를 위한 프로그램이며, 클라이언트/서버 구조로 되어있다. Nethief는 다양한 버전이 존재하며, 해당 보고서에서는 4.9버전을 기준으로 설명을 진행하고자 한다. Nethief는 주로 원격에서 윈도우즈 탐색기 형태로 원격제어를 할 수 있으며, 위의 2개의 관리도구와는 다른 방식으로 서버와 클라이언트 사이의 연결이 진행된다.

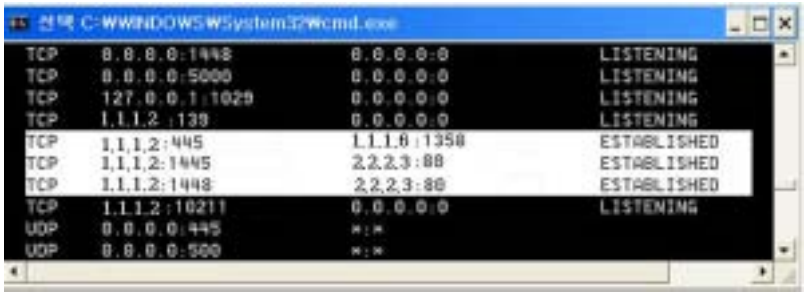


(그림 1-7) Nethief 원격제어 과정

위의 (그림 1-7)은 Nethief 서버와 클라이언트 연결과정의 패킷을 덤프한 것으로써 연결 단계는 아래와 같다.

o 특정 웹서버로부터 TCP 80 (HTTP)로 연결하여 Nethief 관리데몬(Nethief.exe)이 실행중이 시스템에 대한 정보를 가져온다.

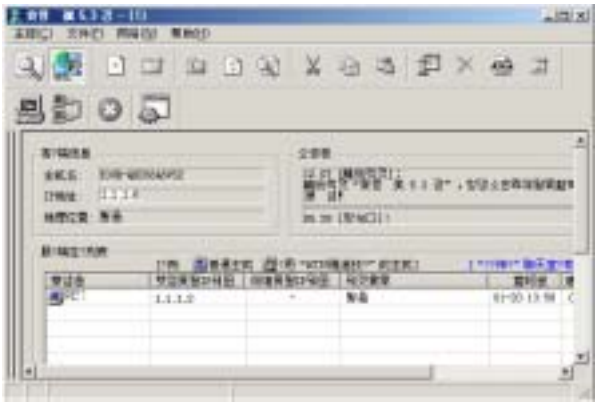
o 위의 그림에서 표시된 영역과 같이 Nethief 관리 클라이언트의 특정포트(TCP 60000)로 원격제어 서버 (Nethief_server.exe)가 연결을 맺는다.



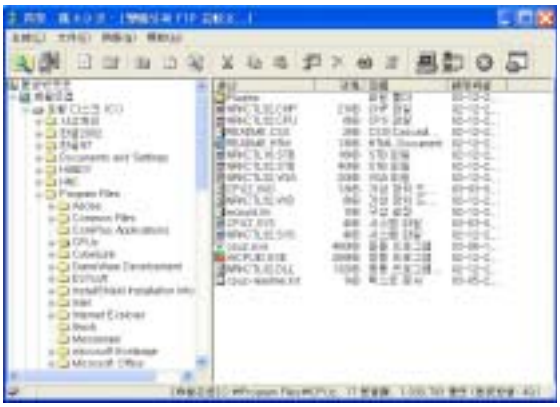
(그림 1-8) Nethief 서버 세션

위의 (그림 1-8)은 Nethief_server.exe가 설치된 경우에 Nethief 관리 클라이언트에 연결된 TCP 하나의 세션과 특정 웹서버에 연결된 여러 세션들을 확인할 수 있다.

일반적으로 해킹 대상 시스템에 원격제어 서버를 설치하고, 해커가 원격제어 클라이언트를 이용하여 특정 포트로 접근하여 명령을 실행하는 반면에, Nethief는 원격제어 서버 역할을 수행하는 Nethief_server.exe가 먼저 해커 시스템의 원격제어 클라이언트인 Nethief.exe에 접속을 한 후, 명령을 전달받아서 실행한다. 이와 같이 원격제어를 위한 연결이 원격제어 서버에서 클라이언트로 진행되기 때문에 해킹을 당한 후에는 개인방화벽으로 방어하기 쉽지 않다.



(그림 1-9) Nethief 관리 클라이언트



(그림 1-10) Nethief 원격제어

위의 (그림 1-9)는 Nethief 관리 클라이언트를 보여주며, Nethief 서버가 설치되 여러 시스템들이 연결되어 있는 것을 확인할 수 있다. (그림 1-10)은 Nethief 관리 클라이언트에서 하나의 원격 시스템을 윈도우즈 탐색기와 같은 GUI형태로 자유롭게 사용할 수 있는 모습을 보여주고 있다.

원격제어 서버인 Nethief_server.exe는 해킹에 사용될 때 IExplorer.exe, Winlog.exe, Svdhosts.exe와 같이 여러 이름으로 변경하고, 실행압축형태로 바꿔서 사용된다. 변형된 실행압축파일을 실행하는 경우 다음과 같은 일들을 수행한다.

① 자신을 윈도우즈 시스템폴더에 복사해 넣는다.
- o Windows 95/98/Me의 경우는 'C:\Windows\System' 폴더에 복사한다.
- o Windows NT/2000의 경우는 'C:\Winnt\System32' 폴더에 복사한다.
- o Windows XP의 경우는 'C:\Windows\System32' 폴더에 복사한다.

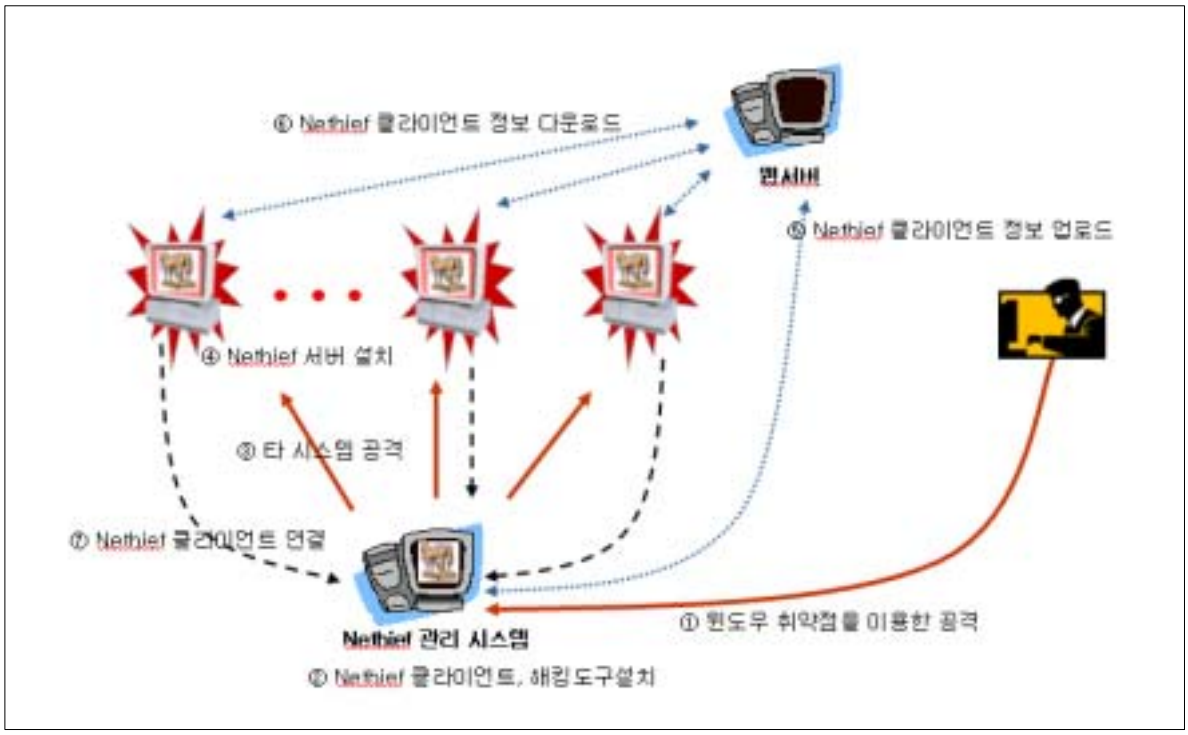
② 피해시스템이 시동될 때 함께 실행되도록 다음의 Registry Key 아래에 등록한다.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
(이하 "Registy Run key"라 한다.)
예) "Internet Explorer" = "IExplorer.exe"

③ 피해시스템은 해커의 중간 연락시스템(해커 컴퓨터가 아니고, 해커의 접속지 주소가 기록된 또 다른 피해시스템)에 접속하여 Nethief.exe의 IP주소와 포트정보를 가져온다. 주로 TCP 80 (HTTP)을 이용하여 이러한 정보를 가져온다.

④ 가져온 해커 시스템의 IP주소와 포트정보를 이용하여 Nethief.exe에 접속한 후, 원격명령을 수행할 수 있는 준비를 완료한다.

3. 침해경로의 이해

여기에서는 관련 침해사고를 분석한 결과, 침해경로에 대해서 설명하고자 한다. 침입자가 공격에 사용한 것으로 추정되는 많은 해킹도구들을 발견할 수 있었으며 이것을 근거로 설명하고자 한다.



(그림 1-11) 침해경로

위의 (그림 1-11)은 침해경로를 보여주고 있으며 각 단계별로 설명하자면 아래와 같다.

① 침입자는 윈도우 취약점을 이용하여 Nethief 관리 시스템으로 사용하고자 하는 시스템을 공격한다.

② 공격 성공 후, 해당 시스템에 Netheif 관리 클라이언트, 다른 백도어(DameWare, Radmin), 해킹도구를 설치한다.

③ 피해시스템을 경유하여 설치된 해킹도구를 이용하여 제 3의 시스템들을 공격한다.

④ 공격 성공 후, 해당 시스템에 Nethiief 서버, 다른 백도어(DameWare, Radmin)을 설치한다.

⑤ Nethief 관리 클라이언트를 시작하여, 해당 시스템의 IP와 서비스 주소를 웹서버에 업로드한다.

⑥ 제 3의 피해시스템들은 Nethief 서버가 Registry Run Key아래에 등록되어 시스템 시작 시 함께 실행되며, 특정 웹서버에서 Nethief 관리 클라이언트의 정보를 다운로드한다.

⑦ 가져온 Nethief 관리 클라이언트의 정보를 이용하여 연결한다.

⑧ 피해시스템들을 이용하여 와레즈(컨텐츠불법유통 사이트)를 운영하거나, 다른 공격에 사용할 수 있다.

4. 해킹피해 사실의 판단 방법

해커는 침투가 완료되면 해당 시스템을 주로 다른 시스템을 공격하기 위한 경유지, Warez에서 영화파일과 같은 데이터의 FTP 서비스, 개인정보 유출과 같은 용도로 이용한다. 침해시스템이 악용되는 과정에서 현상들을 포착하고 다음과 같은 점검을 실시하여 침해사실을 확인해야 한다.

1) 백도어 설치여부 검사

해커는 침해시스템을 악용하기 먼저 원격제어를 위한 DameWare, Radmin, Netheif와 같은 백도어를 설치한다. 여기에서는 DameWare, Radmin 그리고 Nethief의 설치여부를 점검하는 방법을 설명하고자 한다.

각 백도어별 실행파일명, 실행파일위치, 포트번호는 아래의 [표 1-1]과 같다.

[표 1-1] 백도어

	DameWare	Radmin	Nethief
실행파일명	DWSCS.exe	r_admin.exe	Nethief_server.exe IExploer.exe svdhost.exe 등
실행파일위치	윈도우즈 시스템폴더	윈도우즈 시스템폴더	윈도우즈 시스템폴더
포트번호	TCP 6129	TCP 4899	임의의 TCP 포트

해당 백도어의 설치여부를 판단하는 방법은 아래와 같다.

① 각 백도어의 포트번호는 감추기 위해서 변경될 수 있기 때문에 동일한 포트번호가 아닌 경우에도 수상한 포트가 LISTENING, ESTABLISHED, TIME_WAIT인 경우 확인해야 한다.

② 수상한 포트번호를 사용하고 있는 프로세스의 이름과 실행파일의 위치를 확인한다.

③ 의심되는 실행파일을 확인한다. 여기에서 해커가 실행파일의 이름만 변경한 경우에는 해당 실행파일의 아이콘은 변하지 않는다.

④ 해당 실행파일이 윈도우즈 서비스에 등록되어 있는지 확인한다. 윈도우즈 서비스는 아래의 Registry Key 아래에 등록되어 있으므로 Registry 편집기에서 해당 Key아래에서 실행파일명을 조건으로 검색한다.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services (이하 "Registy Service Key"라 한다.)

⑤ 해당 실행파일이 Registry Run Key 아래에 등록되어 있는지 확인한다.

※ 참고 : 일반적으로 원격제어을 위한 백도어 이외에 FTP 서버 프로그램을 설치하는 경우가 많으며, Server-U가 자주 사용된다. 따라서 피해시스템에서 아래의 파일 또한 자주 발견된다.
- o 실행파일명 : ServerUDaemon.exe
- o 실행파일위치 : 윈도우즈 시스템폴더
- o 포트번호 : 사용자 정의

2) 해킹도구 검사

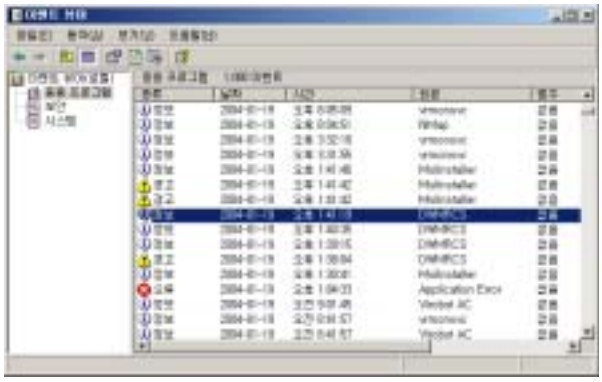
피해시스템에는 해커가 다른 시스템을 공격하는데 사용하기 위해서 해킹도구를 설치하는 경우가 많으며, 해당 파일들은 주로 아래와 같다. 특히 본인이 아래 파일을 설치하지 않았으면 해킹이라고 의심해야 한다.

[표 1-2] 해킹도구

도구명	설 명
Findpass.exe	패스워드를 찾아냄
nbtdump.exe	계정, 공유폴더 등의 정보파일 생성
NC.exe	Command Line 생성
nmap.exe	네트워크를 스캐닝
psexec.exe	원격에서 프로세스 실행
pskill.exe	프로세스 ID 또는 이름을 이용해 프로세스를 종료
pslist.exe	실행중인 프로세스 정보를 보여줌
pwdump4.exe	NT/2000 의 사용자와 패스워드 해쉬를 크랙
ResumeTelnet.exe	텔넷클라이언트

4) 로그 검사

DameWare나 Radmin과 같은 경우 일반적으로 사용되는 원격관리 소프트웨어이므로 Eventlog에 로그를 남기게 되므로 로그를 확인하도록 한다.



(그림 1-12) 이벤트로그 뷰

(그림 1-13) 이벤트로그 상세

위의 (그림 1-12)는 이벤트로그 뷰어를 통해서 DameWare의 로그를 확인하는 것을 보여주고 있다. 이벤트로그 뷰어를 더블 클릭하면 (그림 1-13)과 같은 이벤트 등록정보를 상세하게 볼 수 있으며 이러한 상세 정보에서 본인이 설치하였는지, 언제 설치되었는지를 검토하여 해킹여부를 판별한다.

4. 피해복구 방법

침해사고 시스템을 완벽하게 복구하는 것은 거의 불가능하다. 따라서 운영체제를 다시 설치하는 것을 권장한다. 하지만 재설치가 불가능하거나, 재설치 전에 임시로 운영해야 하는 경우에는 아래의 순서에 따라서 조치하도록 한다.

① 피해시스템 분석에서 발견된 DameWare, Radmin, Nethief와 같은 백도어를 제거한다.
- o 해당 프로세스를 종료시킨다.
- o Fport와 Netsat 명령을 통해서 프로세스 종료를 확인한다.
- o 해당 실행파일을 삭제한다.
- o 윈도우즈 서비스에서 삭제한다.
- o Registry Run Key아래에서 삭제한다.

② 백도어 이외에 FTP도 서비스하지 않으면 위의 백도어 제거방법처럼 제거한다.

③ 해커가 만들어놓은 사용자 계정을 찾아서 삭제하고, 기존의 패스워드를 8자 이상으로 어렵게 만들어서 해킹에 대처한다.

④ 피해시스템 분석에서 발견된 해킹도구 파일들을 제거한다.

5. 예방방법

□ 일반적인 예방방법

1) 패스워드 보안

취약한 패스워드 또는 Null 패스워드를 이용해 DameWare, Radmin, Nethief 등의 프로그램이 설치될 수 있으므로, 사용자들은 정기적으로 컴퓨터의 로그인 패스워드를 변경해야 하며, 본인만이 알 수 있는 문자열로 패스워드를 설정해야 한다. 또한 새롭게 설치한 소프트웨어의 관리 계정의 패스워드가 알기 쉬운 패스워드이거나 NULL 패스워드인 경우가 많으므로, 소프트웨어를 설치할 때는 관련 보안 패치를 함께 설치하고 패스워드도 본인만 알 수 있도록 변경해야한다.

o 패스워드 변경방법
- Windows 2000 : [Ctrl+Alt+Del] ⇨ [암호변경]
- Windows XP : [시작] ⇨ [설정] ⇨ [제어판] ⇨ [사용자계정] ⇨ [계정선택] ⇨ [암호변경]

2) Windwos 보안패치 설치

윈도우즈 운영과정에서 발견되는 취약점들에 대해 MS社에서는 보안 패치를 제공하고 있다. 취약점에 대한 보안 패치가 제대로 적용되지 않았을 경우, 해킹이나 바이러스 감염 등의 피해를 입을 수 있으며, 정상적으로 컴퓨터를 사용하지 못할 수 있으므로 사용자들은 보안 패치를 필수적으로 설치해야 한다.

o 보안취약정보 자동알림기능 설정
- Window운영과정에서 새로운 취약점이 발견될 경우 자동으로 알려주는 기능을 설정하여 취약점을 신속하게 보완한다.
- [시작] ⇨ [제어판] ⇨ [자동 업데이트] ⇨ [알림설정]에서 원하는 항목을 선택.

o Windows 보안패치 설치방법
- [시작] ⇨ [Windows Update]를 선택

3) 최신버전의 백신프로그램으로 점검

대부분 컴퓨터 바이러스나 트로이목마는 백신프로그램으로 점검하면 치료 및 제거할 수 있다. 백신프로그램은 주기적으로 업데이트 하여 신종 바이러스에 대비해야 하며, 반드시 정품 소프트웨어를 사용하여 불법복제 소프트웨어에 묻어올 수 있는 바이러스를 예방해야 한다.

o 백신회사 사이트
- 안철수연구소 : http://www.ahnlab.com
- 하우리 : http://www.hauri.co.kr
- 시만텍 : http://www.symantec.co.kr
- 트랜드마이크로 : http://www.trendmicro.co.kr

4) 방화벽을 통한 보안

Windows 2000/XP에 내장된 방화벽은 외부로부터 들어오는 불법적인 접근을 탐지하고 차단해 준다. 자세한 설정방법은 아래 기술문서를 참고하라.

o Windows 2000/XP에 내장된 방화벽을 통한 보안
- 한글 : http://www.certcc.or.kr ⇨ [기술문서]
- PDF : http://www.certcc.or.kr/paper/tr2003/TR2003_06.pdf

□ 추가적인 예방방법

1) 주기적인 네트워크 상태 점검

'netstat -na' 명령어는 네트워크 포트(TCP, UDP) 상태를 확인함으로써 바이러스나 해킹여부를 진단할 수 있다. 명령어 실행 결과에서 Local 시스템에서 열린 포트를 확인 후 비정상적인 포트나 일반적인 접속이 아닌 접속자의 IP 및 서비스포트를 확인한다.

o 실행방법 : [시작] ⇨ [실행] ⇨ [cmd] ⇨ 'netstat -na' 입력 후 엔터
o 백도어 포트리스트 사이트
http://www.glocksoft.com/trojan_port.htm

2) 실행중인 프로세스 확인

의심가는 프로세스의 CPU 사용량과 메모리 사용량을 확인하고, 악성프로그램도 일반 프로세스명과 비슷하게 변경되어 실행되므로 주의해서 확인한다.

o 실행방법 : [Ctrl+Alt+Del] ⇨ [작업관리자] ⇨ [프로세스]

3) Fport 프로그램을 통한 확인

'netstat -na'와 작업관리자의 프로세스를 통해 의심되는 부분을 확인했다면, Fport 프로그램을 통해 열린 포트와 그와 매칭되는 프로세스를 확인할 수 있다.

o 실행방법 : [시작] ⇨ [실행] ⇨ [cmd] ⇨ [Fport 디렉토리로 이동] ⇨ 'Fport' 입력 후 엔터
o Fport 다운로드 사이트
http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/fport.htm

4) 실행중인 서비스 확인

Windows 시스템은 기본적으로 많은 서비스가 열려 있으므로, 서버 구축 시에 불필요한 서비스는 미리 제거한다. 특히 악성프로그램에 감염되었을 때에도 악성프로그램이 서비스에 등록 될 수 있으므로 주기적으로 점검한다.

o 실행방법 : [시작] ⇨ [프로그램] ⇨ [관리도구] ⇨[컴퓨터관리] ⇨ [서비스]
o 기본 Windows 2000 서비스
http://www.microsoft.com/korea/technet/security/prodtech/windows/windows2000/staysecure/secopsb.asp

5) 사용자 및 공유폴더 확인

o 사용자 확인
현재 생성되어 있는 계정 및 그룹을 확인하여 불법적인 계정이나 일반사용자의 Administroars 그룹 권한 여부 및 불법 그룹의 생성여부를 점검한다. 또한 guest 계정이 '사용안함'으로 되어 있는지 점검한다.
- Windows 2000 : [시작] ⇨ [프로그램] ⇨ [관리도구] ⇨ [컴퓨터관리] ⇨ [로컬 사용자 및 그룹]
- Windows XP : [시작] ⇨ [설정] ⇨ [제어판] ⇨ [사용자 계정]

o 공유폴더 확인
사용자가 공유하지 않은 드라이브 또는 폴더가 있는지 확인한다.
- Windows 2000/XP : [시작] ⇨ [프로그램] ⇨ [관리도구] ⇨ [컴퓨터관리] ⇨ [공유폴더]

6. 참고사이트

1) http://www.microsoft.com/korea
2) http://www.certcc.or.kr/paper/tr2002/tr2002_11/windows_server.pdf