Delivered-To: hans@ubermorgen.com
Date: Thu, 14 Sep 2000 06:49:57 +0200 (CEST)
From: aaron <aaron@lo-res.org>
To: hans@ubermorgen.com
Subject: report of breakin Sep 11th-13th 2000 ubermorgen02.ubermorgen.com (fwd)

---------- Forwarded message ----------
Date: Thu, 14 Sep 2000 06:14:23 +0200 (CEST)
From: aaron <aaron@lo-res.org>
To: cert@cert.org
Cc: max@fastforward.at, aaron@meta.lo-res.org
Subject: report of breakin Sep 11th-13th 2000 ubermorgen02.ubermorgen.com

report of breakin Sep 11th-13th 2000
on ubermorgen02.ubermorgen.com
and attempted break-in at voteauction.com

aaron@meta.lo-res.org

[NOTE: mails to other affected sites / sources of attack will be notified ASAP]

system description:

RedHat Linux 6.2
serving as developers machine, mysql db for ubermorgen.com
(brother machine of voteauction.com which you might have heard of)

IP: 62.116.31.115
server-housed at sil.at (Vienna)

summary report of break-in:

Sep 13th sil.at was informed that many portscans were issued from ubermorgen02 on the 12th in the night to universities, companies, etc. The machine was disconnected from the net next morning. At that time there was no sysadmin with detailed kowledge of the setup of this machine. I started my work recently and have not been involved with detailed setup on ubermorgen02.

On Sep 13th I briefly assessed the damage. No files seemed to be deleted. As a first measure all logins and all services were disabled except telnet from two specific hosts. Passwords were changed. Later it turned out that not only ssh was compromised but also telnetd. So this did not change anything. The machine was re-connected to the net since time was scarce and log files had to be copied to some other place via the net.

As a test a telnet attempt was made to ubermorgen02 while cjm@sil.at (sysadmin at our ISP) watched network traffic on the connected segment. The cracker was logged in again. Obviously the changing of the root password did not help in any way neither did changing /etc/hosts.allow and /etc/hosts.deny

A maybe panic reaction was to issue a shutdown. More detailed file system analysis will be present on Sep 14th evening local time.

We assume that ubermorgen02 was a close enough target to the host voteauction.com which was mentioned in the media recently in the last week(s). voteauction.com is also named ubermorgen03.ubermorgen.com and resides next to ubermorgen02.

Neither can we - at the present stage - 100% assure that other hosts in the ubermorgen.com domain have been compromised but we are fairly sure that this is not the case. It is also possible that the cracker has had root access for some time already.

actions taken on our side
---

this section documents actions which we undertook. Partly this is already described above. on 17:00 pm Sep 12th I got to the console. At that time the machine was taken offline already. I edited /etc/hosts.allow, /etc/hosts.deny as root (described above). Chris Mutter at sil.at (our ISP) discussed matters with me via phone. A maybe panic reaction was to kill off unnessesary processes such as qmail. Then a quick check into

/var/log/* was done revealing what had been going on. I wrote down some IP addresses which were involved at that time. A backup copy of /var was made as /var.bak. Then a "find / -atime +2" and a search on SUID files was done. The first search revealed that /dev/sdc0 was a directory and contained subdirectories such as .lproc and programs for packet sniffing. One of the files revealed that the attacker had been collecting a huge amount of passwords from the net. sil.at provides server-housing for many local customers on this net. The log file was something like 500,000 lines long. At that time everything but telnetd was turned off (see above). Due to time pressure I had to leave and wanted to connect from a specific machine outside. So the targeted pc was re-connected to the net. I left at approx. 19:00 local time.

At approx. 19:30 I telneted in. So did Chris Mutter from sil.at. After realizing the attacker was still present I issued "shutdown -h now" This was at approx. 23:00

technical details of the break-in:

First attempts in the log files which we can see show that he used a buffer overflow attack. modprobe will try to locate a module called <somebinarytexthere>. However this still remains dubious. The second entry is probably DNS related: named (version 8.2.2-P3) is started, eth0 is set to promiscous mode. Then there is a time delay. It is pretty obvious that in the meantime (between Sep 11th 7:41 and Sep 12th 00:30) /var/log/messages entries were deleted manually. .bash_history will hopefully reveal more.
The next wave is an attack on fingerd: connects from different IPs (listed at the end of this section) and ICMP broadcasts are visible. During this wave we can infer that the attacker used quite a few hosts spread around the globe (Israel, US, ...). This attack lasts from approx. 0:30 to 12:00. At this point the attacker has (at the latest) root ssh, telnet and ftp access. We assume that at that point a new version of egcs was installed and a root-toolkit was compiled effectively replacing at least telnetd, sshd, finger, ls, ... with own versions.
At 19:45 the attacker tries to send ICMP source route packets. From then on: lots of finger, ICMP, telnet, ftp and ssh connections.

Since - as said above - the machine has not had proper sysadministration the log entries are rather sparse considered the amount of messages that could have been generated.

More in-depth discussion if technical issues following if neccessary...

Reference: /var/log/messages file

[NOTE: sysadmins at possible sources of attack / possible targets will be notified asap]

```
Sep 10 04:02:00 ubermorgen02 syslogd 1.3-3: restart.
Sep 10 04:02:00 ubermorgen02 syslogd 1.3-3: restart.
Sep 10 04:02:00 ubermorgen02 syslogd 1.3-3: restart.
Sep 10 04:02:00 ubermorgen02 syslogd 1.3-3: restart.
Sep 10 04:02:00 ubermorgen02 syslogd 1.3-3: restart.
Sep 10 04:22:00 ubermorgen02 anacron[9730]: Updated timestamp for job `cron.weekly' to 2000-09-10
Sep 10 04:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 10 04:27:13 ubermorgen02 named[31663]: USAGE 968552833 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 10 04:27:13 ubermorgen02 named[31663]: NSTATS 968552833 967699632
Sep 10 04:27:13 ubermorgen02 named[31663]: XSTATS 968552833 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 10 05:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 10 05:27:13 ubermorgen02 named[31663]: USAGE 968556433 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 10 05:27:13 ubermorgen02 named[31663]: NSTATS 968556433 967699632
Sep 10 05:27:13 ubermorgen02 named[31663]: XSTATS 968556433 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 10 06:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 10 06:27:13 ubermorgen02 named[31663]: USAGE 968560033 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 10 06:27:13 ubermorgen02 named[31663]: NSTATS 968560033 967699632
Sep 10 06:27:13 ubermorgen02 named[31663]: XSTATS 968560033 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 10 07:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 10 07:27:13 ubermorgen02 named[31663]: USAGE 968563633 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 10 07:27:13 ubermorgen02 named[31663]: NSTATS 968563633 967699632
Sep 10 07:27:13 ubermorgen02 named[31663]: XSTATS 968563633 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
```

Weitere Meldungen:

Journale sind erfolgreichste Ö1-Sendungen

Eurosport öffnet Österreichfenster im Web

82 Mio. Europäer haben privaten Internet-Zugang

Deutsche "Nature"-Site startet

meldung

pte000908030
Computer/Telekommunikation, Recht/Steuer

Österreicher versteigert US-Wählerstimmen im Web

Bis zu 100 Dollar für eine Stimme

Sofia (pte, 8. September 00/14:08) - Ein Österreicher hat eine US-amerikanische Web-Seite http://www.**voteauction**.com eines Studenten übernommen, auf der Wählerstimmen für die amerikanische Präsidentenwahl versteigert wurden. Nachdem die Seite letztes Monat in den Vereinigten Staaten vom Netz genommen wurde, hat der Österreicher die Idee aufgegriffen und seinen Server in Bulgarien stationiert, womit er die Zuständigkeit der amerikanischen Behörden ausschaltete.

Für Stimmen von Versteigerern werden angeblich bis zu 100 Dollar geboten. Die Abgabe der richtigen Stimme muss dabei entweder durch Briefwahl oder durch ein Foto des Stimmzettels belegt werden. Teilweise vertraue man aber einfach auf die Ehrlichkeit der Wähler. Der amerikanische Student wollte mit seiner Site ursprünglich in satirischer Form gegen die "plutokratische" amerikanische Gesellschaft protestieren.

Der österreichische Betreiber kann sich vorstellen, Versteigerungen dieser Art auch in Europa anzubieten. Er sehe die amerikanische Wahl als eine Art "Pilotprojekt". Der Kauf einer Stimme auf seiner Website sei schließlich nichts anderes als das Einlösen eines Wahlversprechens eines Kandidaten.
(Ende)

Aussender: pressetext.austria

Redakteur: Oliver Scheiber,
email: scheiber@pressetext.at,
Tel. 01/81140-314

```
Sep 10 08:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 10 08:27:13 ubermorgen02 named[31663]: USAGE 968567233 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 10 08:27:13 ubermorgen02 named[31663]: NSTATS 968567233 967699632
Sep 10 08:27:13 ubermorgen02 named[31663]: XSTATS 968567233 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 10 09:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 10 09:27:13 ubermorgen02 named[31663]: USAGE 968570833 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 10 09:27:13 ubermorgen02 named[31663]: NSTATS 968570833 967699632
Sep 10 09:27:13 ubermorgen02 named[31663]: XSTATS 968570833 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 10 10:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 10 10:27:13 ubermorgen02 named[31663]: USAGE 968574433 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 10 10:27:13 ubermorgen02 named[31663]: NSTATS 968574433 967699632
Sep 10 10:27:13 ubermorgen02 named[31663]: XSTATS 968574433 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 10 11:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 10 11:27:13 ubermorgen02 named[31663]: USAGE 968578033 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 10 11:27:13 ubermorgen02 named[31663]: NSTATS 968578033 967699632
Sep 10 11:27:13 ubermorgen02 named[31663]: XSTATS 968578033 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 10 12:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 10 12:27:13 ubermorgen02 named[31663]: USAGE 968581633 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 10 12:27:13 ubermorgen02 named[31663]: NSTATS 968581633 967699632
Sep 10 12:27:13 ubermorgen02 named[31663]: XSTATS 968581633 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 10 13:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 10 13:27:13 ubermorgen02 named[31663]: USAGE 968585233 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 10 13:27:13 ubermorgen02 named[31663]: NSTATS 968585233 967699632
Sep 10 13:27:13 ubermorgen02 named[31663]: XSTATS 968585233 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 10 14:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 10 14:27:13 ubermorgen02 named[31663]: USAGE 968588833 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 10 14:27:13 ubermorgen02 named[31663]: NSTATS 968588833 967699632
Sep 10 14:27:13 ubermorgen02 named[31663]: XSTATS 968588833 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 10 15:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 10 15:27:13 ubermorgen02 named[31663]: USAGE 968592433 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 10 15:27:13 ubermorgen02 named[31663]: NSTATS 968592433 967699632
Sep 10 15:27:13 ubermorgen02 named[31663]: XSTATS 968592433 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 10 16:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 10 16:27:13 ubermorgen02 named[31663]: USAGE 968596033 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 10 16:27:13 ubermorgen02 named[31663]: NSTATS 968596033 967699632
Sep 10 16:27:13 ubermorgen02 named[31663]: XSTATS 968596033 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 10 17:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 10 17:27:13 ubermorgen02 named[31663]: USAGE 968599633 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 10 17:27:13 ubermorgen02 named[31663]: NSTATS 968599633 967699632
Sep 10 17:27:13 ubermorgen02 named[31663]: XSTATS 968599633 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 10 18:10:07 ubermorgen02 sshd[12728]: log: Connection from 193.220.108.81 port 63024
Sep 10 18:10:59 ubermorgen02 sshd[12728]: log: Password authentication for sofia accepted.
Sep 10 18:13:33 ubermorgen02 sshd[12728]: fatal: Connection closed by remote host.
Sep 10 18:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 10 18:27:13 ubermorgen02 named[31663]: USAGE 968603233 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 10 18:27:13 ubermorgen02 named[31663]: NSTATS 968603233 967699632
Sep 10 18:27:13 ubermorgen02 named[31663]: XSTATS 968603233 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 10 19:05:51 ubermorgen02 sshd[11419]: log: Generating new 768 bit RSA key.
Sep 10 19:05:52 ubermorgen02 sshd[11419]: log: RSA key generation complete.
Sep 10 19:21:10 ubermorgen02 kernel: eth0: Transmit error, Tx status register 82.
Sep 10 19:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 10 19:27:13 ubermorgen02 named[31663]: USAGE 968606833 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 10 19:27:13 ubermorgen02 named[31663]: NSTATS 968606833 967699632
Sep 10 19:27:13 ubermorgen02 named[31663]: XSTATS 968606833 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 10 19:27:41 ubermorgen02 sshd[12833]: log: Connection from 193.220.108.81 port 63260
Sep 10 19:27:58 ubermorgen02 sshd[12833]: log: Password authentication for sofia accepted.
Sep 10 19:28:10 ubermorgen02 sshd[12833]: log: Closing connection to 193.220.108.81
Sep 10 19:30:30 ubermorgen02 kernel: eth0: Transmit error, Tx status register 82.
```

```
Sep 10 19:31:27 ubermorgen02 kernel: eth0: Transmit error, Tx status register 82.
Sep 10 19:33:38 ubermorgen02 last message repeated 2 times
Sep 10 19:37:56 ubermorgen02 last message repeated 3 times
Sep 10 19:41:05 ubermorgen02 kernel: eth0: Transmit error, Tx status register 82.
Sep 10 19:42:06 ubermorgen02 last message repeated 2 times
Sep 10 19:46:23 ubermorgen02 last message repeated 2 times
Sep 10 19:47:57 ubermorgen02 last message repeated 3 times
Sep 10 19:50:43 ubermorgen02 kernel: eth0: Transmit error, Tx status register 82.
Sep 10 19:52:33 ubermorgen02 last message repeated 3 times
Sep 10 19:54:07 ubermorgen02 last message repeated 2 times
Sep 10 19:55:09 ubermorgen02 last message repeated 5 times
Sep 10 19:56:31 ubermorgen02 last message repeated 5 times
Sep 10 19:58:01 ubermorgen02 last message repeated 3 times
Sep 10 19:59:42 ubermorgen02 kernel: eth0: Transmit error, Tx status register 82.
Sep 10 20:01:01 ubermorgen02 last message repeated 2 times
Sep 10 20:02:09 ubermorgen02 last message repeated 4 times
Sep 10 20:03:21 ubermorgen02 last message repeated 2 times
Sep 10 20:03:33 ubermorgen02 last message repeated 2 times
Sep 10 20:05:52 ubermorgen02 sshd[11419]: log: Generating new 768 bit RSA key.
Sep 10 20:05:52 ubermorgen02 sshd[11419]: log: RSA key generation complete.
Sep 10 20:06:15 ubermorgen02 kernel: eth0: Transmit error, Tx status register 82.
Sep 10 20:07:51 ubermorgen02 kernel: eth0: Transmit error, Tx status register 82.
Sep 10 20:09:01 ubermorgen02 last message repeated 3 times
Sep 10 20:10:58 ubermorgen02 last message repeated 3 times
Sep 10 20:12:08 ubermorgen02 last message repeated 5 times
Sep 10 20:17:27 ubermorgen02 kernel: eth0: Transmit error, Tx status register 82.
Sep 10 20:18:52 ubermorgen02 kernel: eth0: Transmit error, Tx status register 82.
Sep 10 20:20:12 ubermorgen02 last message repeated 3 times
Sep 10 20:26:33 ubermorgen02 last message repeated 3 times
Sep 10 20:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 10 20:27:13 ubermorgen02 named[31663]: USAGE 968610433 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 10 20:27:13 ubermorgen02 named[31663]: NSTATS 968610433 967699632
Sep 10 20:27:13 ubermorgen02 named[31663]: XSTATS 968610433 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 10 20:27:29 ubermorgen02 kernel: eth0: Transmit error, Tx status register 82.
Sep 10 20:29:52 ubermorgen02 last message repeated 2 times
Sep 10 20:30:59 ubermorgen02 last message repeated 9 times
Sep 10 20:32:17 ubermorgen02 last message repeated 4 times
Sep 10 20:34:03 ubermorgen02 last message repeated 9 times
Sep 10 20:35:26 ubermorgen02 last message repeated 7 times
Sep 10 20:36:29 ubermorgen02 last message repeated 11 times
Sep 10 20:37:45 ubermorgen02 last message repeated 11 times
Sep 10 20:39:03 ubermorgen02 last message repeated 6 times
Sep 10 20:40:13 ubermorgen02 last message repeated 5 times
Sep 10 20:41:26 ubermorgen02 last message repeated 13 times
Sep 10 20:42:29 ubermorgen02 last message repeated 16 times
Sep 10 20:43:32 ubermorgen02 last message repeated 25 times
Sep 10 20:43:42 ubermorgen02 last message repeated 6 times
Sep 10 21:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 10 21:27:13 ubermorgen02 named[31663]: USAGE 968614033 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 10 21:27:13 ubermorgen02 named[31663]: NSTATS 968614033 967699632
Sep 10 21:27:13 ubermorgen02 named[31663]: XSTATS 968614033 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 10 21:38:22 ubermorgen02 sshd[12948]: log: Connection from 193.220.108.81 port 63431
Sep 10 21:46:06 ubermorgen02 sshd[12948]: log: Password authentication for sofia accepted.
Sep 10 21:57:21 ubermorgen02 sshd[12948]: log: Closing connection to 193.220.108.81
Sep 10 22:05:52 ubermorgen02 sshd[11419]: log: Generating new 768 bit RSA key.
Sep 10 22:05:52 ubermorgen02 sshd[11419]: log: RSA key generation complete.
Sep 10 22:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 10 22:27:13 ubermorgen02 named[31663]: USAGE 968617633 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 10 22:27:13 ubermorgen02 named[31663]: NSTATS 968617633 967699632
Sep 10 22:27:13 ubermorgen02 named[31663]: XSTATS 968617633 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 10 23:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 10 23:27:13 ubermorgen02 named[31663]: USAGE 968621233 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 10 23:27:13 ubermorgen02 named[31663]: NSTATS 968621233 967699632
Sep 10 23:27:13 ubermorgen02 named[31663]: XSTATS 968621233 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 11 00:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 11 00:27:13 ubermorgen02 named[31663]: USAGE 968624833 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 11 00:27:13 ubermorgen02 named[31663]: NSTATS 968624833 967699632
Sep 11 00:27:13 ubermorgen02 named[31663]: XSTATS 968624833 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 11 01:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 11 01:27:13 ubermorgen02 named[31663]: USAGE 968628433 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 11 01:27:13 ubermorgen02 named[31663]: NSTATS 968628433 967699632
Sep 11 01:27:13 ubermorgen02 named[31663]: XSTATS 968628433 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
```

```
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 11 01:56:39 ubermorgen02 kernel: eth0: Transmit error, Tx status register 82.
Sep 11 01:57:44 ubermorgen02 kernel: eth0: Transmit error, Tx status register 82.
Sep 11 02:00:11 ubermorgen02 kernel: eth0: Transmit error, Tx status register 82.
Sep 11 02:02:10 ubermorgen02 last message repeated 2 times
Sep 11 02:03:15 ubermorgen02 kernel: eth0: Transmit error, Tx status register 82.
Sep 11 02:04:22 ubermorgen02 last message repeated 4 times
Sep 11 02:07:12 ubermorgen02 last message repeated 8 times
Sep 11 02:08:05 ubermorgen02 last message repeated 8 times
Sep 11 02:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 11 02:27:13 ubermorgen02 named[31663]: USAGE 968632033 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 11 02:27:13 ubermorgen02 named[31663]: NSTATS 968632033 967699632
Sep 11 02:27:13 ubermorgen02 named[31663]: XSTATS 968632033 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 11 03:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 11 03:27:13 ubermorgen02 named[31663]: USAGE 968635633 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 11 03:27:13 ubermorgen02 named[31663]: NSTATS 968635633 967699632
Sep 11 03:27:13 ubermorgen02 named[31663]: XSTATS 968635633 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 11 04:02:00 ubermorgen02 anacron[13176]: Updated timestamp for job `cron.daily' to 2000-09-11
Sep 11 04:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 11 04:27:13 ubermorgen02 named[31663]: USAGE 968639233 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 11 04:27:13 ubermorgen02 named[31663]: NSTATS 968639233 967699632
Sep 11 04:27:13 ubermorgen02 named[31663]: XSTATS 968639233 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 11 05:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 11 05:27:13 ubermorgen02 named[31663]: USAGE 968642833 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 11 05:27:13 ubermorgen02 named[31663]: NSTATS 968642833 967699632
Sep 11 05:27:13 ubermorgen02 named[31663]: XSTATS 968642833 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 11 06:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 11 06:27:13 ubermorgen02 named[31663]: USAGE 968646433 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 11 06:27:13 ubermorgen02 named[31663]: NSTATS 968646433 967699632
Sep 11 06:27:13 ubermorgen02 named[31663]: XSTATS 968646433 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 11 07:05:18 ubermorgen02 modprobe: modprobe: Can't locate module □Û˘ølo
Sep 11 07:05:18 ubermorgen02 modprobe: modprobe: Can't locate module ^PÙ˘ølo
Sep 11 07:06:35 ubermorgen02 modprobe: modprobe: Can't locate module □Û˘ølo
Sep 11 07:06:35 ubermorgen02 modprobe: modprobe: Can't locate module ^PÙ˘ølo
Sep 11 07:27:13 ubermorgen02 named[31663]: Cleaned cache of 0 RRsets
Sep 11 07:27:13 ubermorgen02 named[31663]: USAGE 968650033 967699632 CPU=0u/0s CHILDCPU=0u/0s
Sep 11 07:27:13 ubermorgen02 named[31663]: NSTATS 968650033 967699632
Sep 11 07:27:13 ubermorgen02 named[31663]: XSTATS 968650033 967699632 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0 SFwdQ=0 SDupQ=0 SErr=0 RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 11 07:31:46 ubermorgen02 named[17249]: starting.  named 8.2.2-P3 Thu Nov 11 01:20:31 EST 1999
^Iroot@porky.devel.redhat.com:/usr/src/bs/BUILD/bind-8.2.2_P3/src/bin/named
Sep 11 07:31:46 ubermorgen02 named[17249]: hint zone "" (IN) loaded (serial 0)
Sep 11 07:31:46 ubermorgen02 named[17249]: Zone "0.0.127.in-addr.arpa" (file named.local): No default TTL set
using SOA minimum instead
Sep 11 07:31:46 ubermorgen02 named[17249]: master zone "0.0.127.in-addr.arpa" (IN) loaded (serial 1997022700)
Sep 11 07:31:46 ubermorgen02 named[17249]: ctl_server: bind: Address already in use
Sep 11 07:31:46 ubermorgen02 named[31663]: ctl_writedone: /var/run/ndc: Broken pipe
Sep 11 07:31:49 ubermorgen02 kernel: eth0: Setting promiscuous mode.
Sep 11 07:32:54 ubermorgen02 syslogd 1.3-3: restart.
Sep 11 07:33:56 ubermorgen02 syslogd 1.3-3: restart.
Sep 11 07:35:46 ubermorgen02 named[17249]: There may be a name server already running on [62.116.31.115].53
Sep 11 07:35:46 ubermorgen02 named[17249]: deleting interface [62.116.31.115].53
Sep 11 07:35:46 ubermorgen02 named[17249]: not listening on any interfaces
Sep 11 07:35:46 ubermorgen02 named[17249]: Forwarding source address is [0.0.0.0].1201
Sep 11 07:35:46 ubermorgen02 named[18096]: Ready to answer queries.
Sep 11 07:38:10 ubermorgen02 PAM_pwdb[18101]: (su) session opened for user dev by (uid=0)
Sep 11 07:40:04 ubermorgen02 PAM_pwdb[18101]: (su) session closed for user dev
Sep 11 07:40:53 ubermorgen02 modprobe: modprobe: Can't locate module □Û˘ølo
Sep 11 07:40:53 ubermorgen02 modprobe: modprobe: Can't locate module ^PÙ˘ølo
Sep 11 07:41:17 ubermorgen02 named[18236]: starting.  named 8.2.2-P3 Thu Nov 11 01:20:31 EST 1999
^Iroot@porky.devel.redhat.com:/usr/src/bs/BUILD/bind-8.2.2_P3/src/bin/named
Sep 11 07:41:17 ubermorgen02 named[18236]: hint zone "" (IN) loaded (serial 0)
Sep 11 07:41:17 ubermorgen02 named[18236]: Zone "0.0.127.in-addr.arpa" (file named.local): No default TTL set
using SOA minimum instead
Sep 11 07:41:17 ubermorgen02 named[18236]: master zone "0.0.127.in-addr.arpa" (IN) loaded (serial 1997022700)
Sep 11 07:41:17 ubermorgen02 named[18236]: ctl_server: bind: Address already in use
Sep 11 07:41:19 ubermorgen02 kernel: eth0: Setting promiscuous mode.
Sep 12 00:30:21 ubermorgen02 syslogd 1.3-3: restart.
Sep 12 00:30:32 ubermorgen02 syslogd 1.3-3: restart.
Sep 12 00:30:41 ubermorgen02 syslogd 1.3-3: restart.
```

```
Sep 12 00:42:15 ubermorgen02 named[18591]: Cleaned cache of 0 RRsets
Sep 12 00:42:15 ubermorgen02 named[18591]: USAGE 968712135 968650935 CPU=0u/0.01s CHILDCPU=0u/0s
Sep 12 00:42:15 ubermorgen02 named[18591]: NSTATS 968712135 968650935 TXT=1
Sep 12 00:42:15 ubermorgen02 named[18591]: XSTATS 968712135 968650935 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=1 SFwdQ=0 SDupQ=0 SErr=0 RQ=1 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 12 01:10:34 ubermorgen02 in.fingerd[26685]: connect from 199.34.28.91
Sep 12 01:10:37 ubermorgen02 in.fingerd[26687]: connect from 216.144.137.67
Sep 12 01:42:15 ubermorgen02 named[18591]: Cleaned cache of 0 RRsets
Sep 12 01:42:15 ubermorgen02 named[18591]: USAGE 968715735 968650935 CPU=0u/0.01s CHILDCPU=0u/0s
Sep 12 01:42:15 ubermorgen02 named[18591]: NSTATS 968715735 968650935 TXT=1
Sep 12 01:42:15 ubermorgen02 named[18591]: XSTATS 968715735 968650935 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=1 SFwdQ=0 SDupQ=0 SErr=0 RQ=1 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 12 01:42:38 ubermorgen02 in.fingerd[26927]: connect from 62.136.74.195
Sep 12 01:45:39 ubermorgen02 in.fingerd[26949]: connect from 216.145.17.179
Sep 12 02:06:39 ubermorgen02 kernel: 212.143.104.169 sent an invalid ICMP error to a broadcast.
Sep 12 02:06:39 ubermorgen02 kernel: 212.143.104.181 sent an invalid ICMP error to a broadcast.
Sep 12 02:07:04 ubermorgen02 kernel: 212.143.106.89 sent an invalid ICMP error to a broadcast.
Sep 12 02:07:48 ubermorgen02 kernel: 212.143.110.53 sent an invalid ICMP error to a broadcast.
Sep 12 02:17:17 ubermorgen02 kernel: eth0: Transmit error, Tx status register 82.
Sep 12 02:17:48 ubermorgen02 last message repeated 2 times
Sep 12 02:19:12 ubermorgen02 last message repeated 5 times
Sep 12 02:20:33 ubermorgen02 last message repeated 4 times
Sep 12 02:21:51 ubermorgen02 last message repeated 3 times
Sep 12 02:22:56 ubermorgen02 last message repeated 8 times
Sep 12 02:23:33 ubermorgen02 last message repeated 10 times
Sep 12 02:32:46 ubermorgen02 kernel: 216.145.200.1 sent an invalid ICMP error to a broadcast.
Sep 12 02:42:15 ubermorgen02 named[18591]: Cleaned cache of 0 RRsets
Sep 12 02:42:15 ubermorgen02 named[18591]: USAGE 968719335 968650935 CPU=0u/0.01s CHILDCPU=0u/0s
Sep 12 02:42:15 ubermorgen02 named[18591]: NSTATS 968719335 968650935 TXT=1
Sep 12 02:42:15 ubermorgen02 named[18591]: XSTATS 968719335 968650935 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=1 SFwdQ=0 SDupQ=0 SErr=0 RQ=1 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 12 03:06:43 ubermorgen02 sshd[27362]: log: Connection from 193.220.108.81 port 62298
Sep 12 03:08:48 ubermorgen02 sshd[27362]: log: Password authentication for sofia accepted.
Sep 12 03:42:15 ubermorgen02 named[18591]: Cleaned cache of 0 RRsets
Sep 12 03:42:15 ubermorgen02 named[18591]: USAGE 968722935 968650935 CPU=0u/0.01s CHILDCPU=0u/0s
Sep 12 03:42:15 ubermorgen02 named[18591]: NSTATS 968722935 968650935 TXT=1
Sep 12 03:42:15 ubermorgen02 named[18591]: XSTATS 968722935 968650935 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=1 SFwdQ=0 SDupQ=0 SErr=0 RQ=1 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 12 04:02:00 ubermorgen02 anacron[27559]: Updated timestamp for job `cron.daily' to 2000-09-12
Sep 12 04:05:55 ubermorgen02 sshd[11419]: log: Generating new 768 bit RSA key.
Sep 12 04:05:55 ubermorgen02 sshd[11419]: log: RSA key generation complete.
Sep 12 04:13:42 ubermorgen02 in.fingerd[27710]: connect from 212.137.215.239
Sep 12 04:13:55 ubermorgen02 in.fingerd[27712]: connect from 212.137.215.239
Sep 12 04:42:15 ubermorgen02 named[18591]: Cleaned cache of 0 RRsets
Sep 12 04:42:15 ubermorgen02 named[18591]: USAGE 968726535 968650935 CPU=0u/0.01s CHILDCPU=0u/0s
Sep 12 04:42:15 ubermorgen02 named[18591]: NSTATS 968726535 968650935 TXT=1
Sep 12 04:42:15 ubermorgen02 named[18591]: XSTATS 968726535 968650935 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=1 SFwdQ=0 SDupQ=0 SErr=0 RQ=1 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 12 05:28:33 ubermorgen02 in.fingerd[27862]: connect from 212.141.91.161
Sep 12 05:28:59 ubermorgen02 in.fingerd[27864]: connect from 212.141.91.161
Sep 12 05:29:08 ubermorgen02 in.fingerd[27866]: connect from 212.141.91.161
Sep 12 05:29:27 ubermorgen02 in.ntalkd[27868]: connect from 212.141.91.161
Sep 12 05:29:28 ubermorgen02 talkd[27868]: 212.141.91.161: bad dns
Sep 12 05:29:31 ubermorgen02 last message repeated 2 times
Sep 12 05:29:31 ubermorgen02 talkd[27868]: recvfrom: Connection refused
Sep 12 05:33:59 ubermorgen02 sshd[27362]: fatal: Read error from remote host: Connection reset by peer
Sep 12 05:42:15 ubermorgen02 named[18591]: Cleaned cache of 0 RRsets
Sep 12 05:42:15 ubermorgen02 named[18591]: USAGE 968730135 968650935 CPU=0u/0.01s CHILDCPU=0u/0s
Sep 12 05:42:15 ubermorgen02 named[18591]: NSTATS 968730135 968650935 TXT=1
Sep 12 05:42:15 ubermorgen02 named[18591]: XSTATS 968730135 968650935 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=1 SFwdQ=0 SDupQ=0 SErr=0 RQ=1 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 12 05:59:49 ubermorgen02 in.fingerd[28182]: connect from 216.148.253.10
Sep 12 05:59:49 ubermorgen02 in.fingerd[28183]: connect from 216.148.253.10
Sep 12 05:59:49 ubermorgen02 in.fingerd[28186]: connect from 216.148.253.10
Sep 12 05:59:49 ubermorgen02 in.fingerd[28185]: connect from 216.148.253.10
Sep 12 05:59:49 ubermorgen02 in.fingerd[28184]: connect from 216.148.253.10
Sep 12 05:59:49 ubermorgen02 in.fingerd[28187]: connect from 216.148.253.10
Sep 12 05:59:50 ubermorgen02 in.fingerd[28188]: connect from 216.148.253.10
Sep 12 05:59:50 ubermorgen02 in.fingerd[28189]: connect from 216.148.253.10
Sep 12 05:59:50 ubermorgen02 in.fingerd[28200]: connect from 216.148.253.10
Sep 12 05:59:50 ubermorgen02 in.fingerd[28199]: connect from 216.148.253.10
Sep 12 05:59:50 ubermorgen02 in.fingerd[28190]: connect from 216.148.253.10
Sep 12 05:59:50 ubermorgen02 in.fingerd[28201]: connect from 216.148.253.10
Sep 12 05:59:50 ubermorgen02 in.fingerd[28202]: connect from 216.148.253.10
Sep 12 05:59:50 ubermorgen02 in.fingerd[28203]: connect from 216.148.253.10
Sep 12 05:59:50 ubermorgen02 in.fingerd[28211]: connect from 216.148.253.10
```

```
Sep 12 05:59:50 ubermorgen02 in.fingerd[28209]: connect from 216.148.253.10
Sep 12 05:59:50 ubermorgen02 in.fingerd[28213]: connect from 216.148.253.10
Sep 12 05:59:50 ubermorgen02 in.fingerd[28210]: connect from 216.148.253.10
Sep 12 05:59:50 ubermorgen02 in.fingerd[28212]: connect from 216.148.253.10
Sep 12 05:59:50 ubermorgen02 in.fingerd[28216]: connect from 216.148.253.10
Sep 12 05:59:53 ubermorgen02 in.fingerd[28221]: connect from 216.148.253.10
Sep 12 05:59:54 ubermorgen02 in.fingerd[28224]: connect from 216.148.253.10
Sep 12 06:00:50 ubermorgen02 in.fingerd[28231]: connect from 216.148.253.10
Sep 12 06:00:50 ubermorgen02 in.fingerd[28232]: connect from 216.148.253.10
Sep 12 06:00:50 ubermorgen02 in.fingerd[28233]: connect from 216.148.253.10
Sep 12 06:42:15 ubermorgen02 named[18591]: Cleaned cache of 0 RRsets
Sep 12 06:42:15 ubermorgen02 named[18591]: USAGE 968733735 968650935 CPU=0u/0.01s CHILDCPU=0u/0s
Sep 12 06:42:15 ubermorgen02 named[18591]: NSTATS 968733735 968650935 TXT=1
Sep 12 06:42:15 ubermorgen02 named[18591]: XSTATS 968733735 968650935 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=1 SFwdQ=0 SDupQ=0 SErr=0 RQ=1 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 12 07:42:15 ubermorgen02 named[18591]: Cleaned cache of 0 RRsets
Sep 12 07:42:15 ubermorgen02 named[18591]: USAGE 968737335 968650935 CPU=0u/0.01s CHILDCPU=0u/0s
Sep 12 07:42:15 ubermorgen02 named[18591]: NSTATS 968737335 968650935 TXT=1
Sep 12 07:42:15 ubermorgen02 named[18591]: XSTATS 968737335 968650935 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=1 SFwdQ=0 SDupQ=0 SErr=0 RQ=1 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 12 08:42:15 ubermorgen02 named[18591]: Cleaned cache of 0 RRsets
Sep 12 08:42:15 ubermorgen02 named[18591]: USAGE 968740935 968650935 CPU=0u/0.01s CHILDCPU=0u/0s
Sep 12 08:42:15 ubermorgen02 named[18591]: NSTATS 968740935 968650935 TXT=1
Sep 12 08:42:15 ubermorgen02 named[18591]: XSTATS 968740935 968650935 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=1 SFwdQ=0 SDupQ=0 SErr=0 RQ=1 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 12 08:50:32 ubermorgen02 kernel: 194.151.237.26 sent an invalid ICMP error to a broadcast.
Sep 12 08:50:32 ubermorgen02 kernel: 194.151.237.30 sent an invalid ICMP error to a broadcast.
Sep 12 08:50:32 ubermorgen02 kernel: 194.151.237.38 sent an invalid ICMP error to a broadcast.
Sep 12 08:50:33 ubermorgen02 kernel: 194.151.237.102 sent an invalid ICMP error to a broadcast.
Sep 12 08:50:34 ubermorgen02 kernel: 194.151.237.110 sent an invalid ICMP error to a broadcast.
Sep 12 09:22:57 ubermorgen02 in.fingerd[16560]: connect from 194.152.111.82
Sep 12 09:42:15 ubermorgen02 named[18591]: Cleaned cache of 0 RRsets
Sep 12 09:42:15 ubermorgen02 named[18591]: USAGE 968744535 968650935 CPU=0u/0.01s CHILDCPU=0u/0s
Sep 12 09:42:15 ubermorgen02 named[18591]: NSTATS 968744535 968650935 TXT=1
Sep 12 09:42:15 ubermorgen02 named[18591]: XSTATS 968744535 968650935 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=1 SFwdQ=0 SDupQ=0 SErr=0 RQ=1 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 12 10:42:15 ubermorgen02 named[18591]: Cleaned cache of 0 RRsets
Sep 12 10:42:15 ubermorgen02 named[18591]: USAGE 968748135 968650935 CPU=0u/0.01s CHILDCPU=0u/0s
Sep 12 10:42:15 ubermorgen02 named[18591]: NSTATS 968748135 968650935 TXT=1
Sep 12 10:42:15 ubermorgen02 named[18591]: XSTATS 968748135 968650935 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=1 SFwdQ=0 SDupQ=0 SErr=0 RQ=1 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 12 10:49:49 ubermorgen02 in.telnetd[17722]: connect from 194.153.198.71
Sep 12 10:50:16 ubermorgen02 login[17723]: invalid password for `UNKNOWN' on `pts/4' from `194.153.198.71'
Sep 12 10:50:23 ubermorgen02 inetd[18249]: pid 17722: exit status 1
Sep 12 11:42:15 ubermorgen02 named[18591]: Cleaned cache of 0 RRsets
Sep 12 11:42:15 ubermorgen02 named[18591]: USAGE 968751735 968650935 CPU=0u/0.01s CHILDCPU=0u/0s
Sep 12 11:42:15 ubermorgen02 named[18591]: NSTATS 968751735 968650935 TXT=1
Sep 12 11:42:15 ubermorgen02 named[18591]: XSTATS 968751735 968650935 RR=1 RNXD=0 RFwdR=0 RDupR=0 RFail=0
RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=1 SFwdQ=0 SDupQ=0 SErr=0 RQ=1 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0
SFwdR=0 SFail=0 SFErr=0 SNaAns=0 SNXD=0
Sep 12 12:02:33 ubermorgen02 in.ftpd[18142]: connect from 216.154.119.29
Sep 12 12:02:33 ubermorgen02 sshd[18143]: log: Connection from 216.154.119.29 port 2301
Sep 12 12:02:33 ubermorgen02 in.telnetd[18144]: connect from 216.154.119.29
Sep 12 12:02:34 ubermorgen02 telnetd[18144]: ttloop: peer died: EOF
Sep 12 12:02:34 ubermorgen02 inetd[18249]: pid 18144: exit status 1
Sep 12 12:02:34 ubermorgen02 in.fingerd[18145]: connect from 216.154.119.29
Sep 12 12:02:34 ubermorgen02 inetd[18249]: pid 18145: exit status 1
Sep 12 12:02:35 ubermorgen02 sshd[18143]: fatal: Did not receive ident string.
Sep 12 12:02:37 ubermorgen02 inetd[18249]: pid 18146: exit status 1
Sep 12 12:02:38 ubermorgen02 ftpd[18142]: FTP session closed
Sep 12 12:03:23 ubermorgen02 sshd[18147]: log: Connection from 216.154.119.29 port 3325
Sep 12 12:03:23 ubermorgen02 in.telnetd[18148]: connect from 216.154.119.29
Sep 12 12:03:23 ubermorgen02 in.ftpd[18149]: connect from 216.154.119.29
Sep 12 12:03:23 ubermorgen02 telnetd[18148]: ttloop: peer died: EOF
Sep 12 12:03:23 ubermorgen02 inetd[18249]: pid 18148: exit status 1
Sep 12 12:03:23 ubermorgen02 sshd[18147]: fatal: Did not receive ident string.
Sep 12 12:03:23 ubermorgen02 in.fingerd[18151]: connect from 216.154.119.29
Sep 12 12:03:23 ubermorgen02 inetd[18249]: pid 18151: exit status 1
Sep 12 12:03:23 ubermorgen02 ftpd[18149]: FTP session closed
Sep 12 12:03:24 ubermorgen02 inetd[18249]: pid 18150: exit status 1
Sep 12 12:04:40 ubermorgen02 kernel: 194.154.246.22 sent an invalid ICMP error to a broadcast.
Sep 12 12:05:55 ubermorgen02 sshd[11419]: log: Generating new 768 bit RSA key.
Sep 12 12:05:56 ubermorgen02 sshd[11419]: log: RSA key generation complete.
Sep 12 12:29:41 ubermorgen02 kernel: 216.155.19.230 sent an invalid ICMP error to a broadcast.
Sep 12 12:42:15 ubermorgen02 named[18591]: Cleaned cache of 0 RRsets
Sep 12 12:42:15 ubermorgen02 named[18591]: USAGE 968755335 968650935 CPU=0u/0.01s CHILDCPU=0u/0s
Sep 12 12:42:15 ubermorgen02 named[18591]: NSTATS 968755335 968650935 TXT=1
```