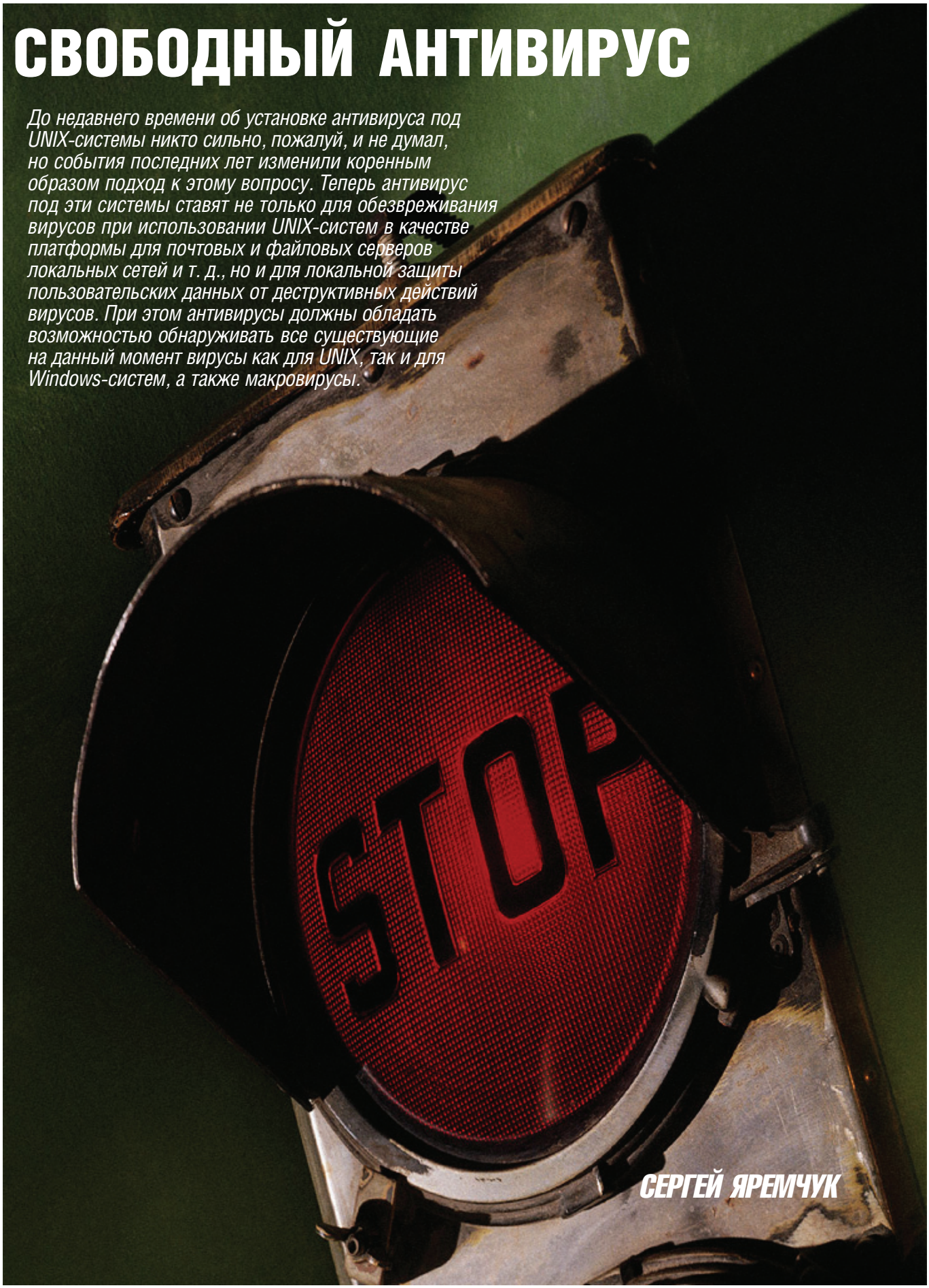
СВОБОДНЫЙ АНТИВИРУС

До недавнего времени об установке антивируса под UNIX-системы никто сильно, пожалуй, и не думал, но события последних лет изменили коренным образом подход к этому вопросу. Теперь антивирус под эти системы ставят не только для обезвреживания вирусов при использовании UNIX-систем в качестве платформы для почтовых и файловых серверов локальных сетей и т. д., но и для локальной защиты пользовательских данных от деструктивных действий вирусов. При этом антивирусы должны обладать возможностью обнаруживать все существующие на данный момент вирусы как для UNIX, так и для Windows-систем, а также макровирусы.



СЕРГЕЙ ЯРЕМЧУК

Наибольшей популярностью среди антивирусов пользуется DrWeb от ЗАО «ДиалогНаука»: http://www.drweb.ru, обладающий действительно хорошими характеристиками и эвристическим анализатором, позволяющим иногда обнаружить неизвестный вирус. Все, в общем, хорошо, но, собрав полностью сервер из бесплатных компонентов, выбить финансы для того, чтобы платить за лицензию, под конец года не получилось. А ограничения ознакомительной версии, в частности невозможность проверки архивов, мне не совсем подходят. Плюс зацикливание на одном продукте обычно мешает увидеть его слабые и сильные стороны, все, как говорится, познается в сравнении. Тем более что в Интернете я постоянно натыкался на другие антивирусы, и мне захотелось поискать замену (или убедиться в отсутствии таковой, что тоже хорошо). В результате я вышел на несколько довольно интересных проектов, о которых речь пойдет в этой и следующей статьях.

Clam AntiVirus (http://clamav.sourceforge.net/ или http://www.clamav.net/) представляет собой антивирусный комплект для UNIX-систем. Главная цель продукта – интеграция с почтовыми серверами для проверки вложений на предмет наличия вирусов. В настоящий момент поддерживается широкий спектр операционных систем: Linux, Solaris, FreeBSD, OpenBSD, NetBSD, AIX, Mac OS X, BeOS, HPUX, SCO UNIX и Windows/Cygwin на нескольких архитектурах: Intel, Alpha, Sparc, Cobalt MIPS boxes, PowerPC, RISC 6000, что уже вызывает уважение. Распространяется по лицензии GPL, POSIX-интерфейс и общедоступные библиотеки позволяют быстро адаптировать его с другими приложениями. Работает с архивами и сжатыми файлами, в настоящее время встроена поддержка RAR, Zip, Gzip, Bzip2. Также встроена поддержка защиты от mail-бомб, которые периодически любят закидывать в пользовательские ящики, и поддерживается milter-интерфейс к программе Sendmail. Обнаруживает, по данным разработчиков, более 20 000 вирусов, червей и троянов (хотя программа при запуске выдает сообщение о чуть больше 10 000, остальное в дополнительных базах). Конечно, по сравнению с другими подобными продуктами число получилось небольшое, но ведь мы знаем, что количество можно считать по-разному, хотя сама программа при запуске выдает сообщение о 10 000 вирусов. При необходимости можно воспользоваться он-лайн-сканером, позволяющим протестировать файлы на жестком диске. Для этого заходим по адресу: http://www.gietl.com/test-clamav и указываем на файл. Если же вы имеете вирус, который не обнаруживается ClamAV с обновленными базами, то по адресу: http://www.nervous.it/~nervous/cgi-bin/sendvirus.cgi или http://www.clamav.net/cgi-bin/sendvirus.cgi можно заполнить форму, где нужно обязательно указать свой e-mail, имя и место расположения зараженного файла, опционально можно также проставить антивирус, обнаруживший заразу. Другой вариант: послать zip-архив с паролем virus по адресу virus@clamav.net. После чего вирус будет проанализирован и добавлен в базу данных. Об остальных возможностях поговорим, когда посмотрим на его работу в действии.

Установка

Из библиотек требуются zlib и bzip2, которые имеются в большинстве систем. Если привычнее пользоваться уже скомпилированными пакетами, то зайдите на страницу http://clamav.sourceforge.net/binary.html и выберите нужную ссылку: на момент написания статьи это Debian, RedHat – Fedora, PLD (Polish(ed) Linux Distribution), Mandrake, AIX, FreeBSD, OpenBSD и MS Windows, на установке в этом случае останавливаться не буду. В остальных случаях нужно компилировать самому, хотя ничего особо сложного разработчики не придумали.

```
#tar xzvf clamav-0.65.tar.gz
# cd clamav-0.65
```

Единственная задержка возникает при конфигурировании и выглядит это так:

```
#./configure
...
/dev/(u)random detected.
Checking /etc/passwd...
ERROR: User "clamav" (and/or group "clamav") doesn't exist.
Please create it. You can omit this check with the --disable-
clamav option.
```

Дело в том, что разработчики в целях безопасности рекомендуют запускать утилиту от лица пользователя clamav, а не root, и не устанавливать ни в коем случае SUID или SGID.

Избежать этого сообщения можно двумя способами: добавить параметр --disable-clamav при конфигурировании или просто создать этого пользователя.

```
# groupadd clamav
# useradd -g clamav -s /bin/false -c "Clam AntiVirus" clamav
```

По умолчанию ClamAV устанавливается в /usr/local, и, соответственно, конфигурационный файл будет лежать в /usr/local/etc, его месторасположение на /etc можно изменить, добавив опцию --sysconfdir=/etc.

Если конфигурирование завершилось без ошибок, компилируем и устанавливаем.

```
# make
# su -c "make install"
```

После окончания установки в нашем распоряжении будет несколько исполняемых файлов:

- clamscan – утилита командной строки, предназначенная для проверки файлов и каталогов на предмет наличия вирусов.
- clamd – антивирусный демон, прослушивающий подключения к UNIX или TCP-сокетам и сканирующий каталоги по требованию. Обеспечена возможность on-access просмотра (только Linux) при применении утилиты clamuko.
- clamdscan – простой интерфейс к демону clamd, позволяет также сканировать файлы и каталоги, при этом используются те же параметры, что и в clamscan, и может полностью заменить clamscan.
- clamav-milter (при конфигурировании с опцией --enable-milter) – представляет собой антивирусный интерфейс к sendmail, использует для просмотра почты clamd.

- freshclam – утилита автоматического обновления вирусной базы данных через Интернет, позволяющая держать ее в самом современном состоянии.
- sigtool – генерирует вирусную сигнатуру, используя внешний антивирусный сканер, который способен обнаружить вирус. Может создавать шестнадцатиричный дамп и формировать и распаковывать CVD-базу данных (ClamAV Virus Database).

Теперь по порядку и поподробней. Проверить текущий каталог на наличие вирусов можно, просто набрав clamscan без каких-либо параметров. В результате получим список проверенных файлов и отчет. Список просканированных файлов позволяет проверить работу утилиты с различными типами файлов на начальном этапе, но в большинстве случаев лучше добавить параметр -i для вывода только зараженных файлов. Указать на файлы, находящиеся в другом каталоге, можно, перечислив их в строке запуска, или, если проверяется каталог, то указать путь к нему, не забыв опцию -r для рекурсивного обхода (для проверки работы антивируса с пакетом поставляется несколько тестовых файлов).

```
# /usr/local/bin/clamscan -r -i /home/sergej/work/clamav-0.65/
```

```
/home/sergej/work/clamav-0.65//test/test1: ClamAV-Test-Signature FOUND
/home/sergej/work/clamav-0.65//test/test1.bz2: ClamAV-Test-Signature FOUND
/home/sergej/work/clamav-0.65//test/test2.zip: ClamAV-Test-Signature FOUND
/home/sergej/work/clamav-0.65//test/test3.rar: ClamAV-Test-Signature FOUND
/home/sergej/work/clamav-0.65//test/test2.badext: ClamAV-Test-Signature FOUND

———— SCAN SUMMARY ————
Known viruses: 10131
Scanned directories: 42
Scanned files: 390
Infected files: 5
Data scanned: 4.49 MB
I/O buffer size: 131072 bytes
Time: 7.204 sec (0 m 7 s)
```

Опция --database= позволяет указать место расположения дополнительной антивирусной базы. Также по умолчанию программа не ведет никаких логов, при работе с cron это не совсем удобно, т.к. теряется контроль над работой программы, при помощи --log= можно указать, в какой файл их заносить. При необходимости проверки отдельных файлов каталога можно воспользоваться опциями --exclude=PATT и -include=PATT. Первая позволяет указать шаблоны файлов, которые не надо проверять, а вторая, наоборот, только те, которые надо просканировать в поиске вирусов. Опция -mbox включает сканирование почтовых каталогов и файлов.

```
#clamscan -r --mbox /var/spool/mail
```

Или можно проверять выход другой программы на наличие вирусов.

```
#cat testfile | clamscan -
```

Кроме вывода информации об обнаружении вируса можно удалить (--remove) или переместить (--move=DIRECTORY) такие файлы в другой каталог. Обычно при работе с архивами программа сама находит нужную утилиту для распаковки, и дополнительных указаний ей не надо, но если появляются сообщения вроде:

```
/mnt/test/test.zip: Zip module failure
```

то указываем на необходимость проверки архивов, и если не видно нужного архиватора в переменной $PATH, то указываем также местонахождение такой программы. Например, для rar: -unrar[=FULLPATH]. Так, для zip-архива строка запуска может выглядеть так:

```
# clamscan -unzip /mnt/test/test.zip
```

После чего программа должна вывести список всех файлов архива с результатами проверки. И еще одна проблема может подстерегать при проверке архивов. Выглядит она так.

```
Write error (disk full?). Continue? (y/n/^C)
```

Каталог /tmp забивается таким образом очень быстро, т.е., закинув большой архив, можно провести DOS-атаку. Чтобы избежать этого, можно указать при помощи -tempdir= на другой каталог, в котором побольше свободного места, или установив максимальное количество извлекаемых за один раз файлов (-max-files=#n), или извлечь сначала #n Кб архива (использовав nM или nm, можно указать на количество Мб) при помощи –max-space=#n. Можно просто указать на максимальный уровень рекурсии обхода архива: -max-recursion=#n.

В следующем примере используем новую антивирусную базу и ограничиваем размер временных файлов в 50 Мб, плюс проверяем архивы.

```
#clamscan -d /tmp/newclamdb -tgz -deb -unrar ↵
    --max-space=50m -r /home
```

Я надеюсь, по clamscan все понятно. Переходим к демону clamd. Главное отличие демона от сканера заключается в том, что он один раз при старте загружает все необходимые базы и настройки и находится в оперативной памяти постоянно готовым выполнить работу. В своей работе он использует конфигурационный файл clamav.conf. Если запустить программу без дополнительного редактирования (в том случае, если установка происходила из исходных текстов), то демон откажется работать.

```
#  /usr/local/sbin/clamd
```

```
ERROR: Please edit the example config file /usr/local/etc/clamav.conf.
ERROR: Can't parse the config file /usr/local/etc/clamav.conf
```

Файл хорошо комментирован, и опции описаны в man, чтобы заставить работать демон в конфигурации по умолчанию, достаточно убрать или закомментировать строку Example в самом начале файла. Пример (ненужные параметры достаточно закомментировать):

```
#Example
# Путь к лог-файлу
LogFile  /var/log/clamav/clamd.log
# Блокировка записи в лог-файл (необходима при запуске
# нескольких демонов одновременно)в том числе и во избежание
# работы с одинаковой конфигурацией
#LogFileUnlock
```

```
# максимальный размер лог-файла (0 - без ограничений)
LogFileMaxSize 0
# Использование syslog
LogSyslog
# Подробный отчет
#LogVerbose
# Файл для сохранения идентификатора процесса
PidFile /var/run/clamav/clamd.pid
# Путь к антивирусным базам (по умолчанию /usr/local/share/clamav)
DataDirectory /var/lib/clamav
# Демон может работать в сетевом или локальном режиме,
# в целях безопасности рекомендуется пока последний, но вот
# посылать сигналы мне показалось более удобным именно
# в сетевом. Несколько следующих строк необходимы для
# настройки сетевого режима.
#LocalSocket /var/run/clamav/clamd.sock
#FixStaleSocket
#TCPSocket 3310
#TCPAddr 127.0.0.1
#MaxConnectionQueueLength 30
# Предварительная запись потока
StreamSaveToDisk
# Предел для потока, после которого соединение закрывается
#StreamMaxLength 10M
# Максимальное количество одновременно выполняемых задач
MaxThreads 10
# Максимальная рекурсия каталога
MaxDirectoryRecursion 15
# Следование символическим ссылкам для каталогов и файлов
#FollowDirectorySymlinks
#FollowFileSymlinks
# Проверка целостности баз (по умолчанию 1 час)
#SelfCheck 600
# Команда, которая должна выполниться при обнаружении вируса.
# При этом используются подстановки %f - имя инфицированного
# файла, %v - название вируса. Должен использоваться полный
# путь к команде
#VirusEvent /usr/local/bin/send_sms 123456789 "VIRUS ALERT: %f: %v"
# Имя пользователя, от которого запускается демон, он должен
# иметь права на изменение всех перечисленных файлов и каталогов.
User clamav
# Работа с почтой и архивами, для RAR нужна отдельная строка
ScanMail
ScanArchive
ScanRAR
# Установка максимальных значений для архивов для защиты
# от mail-бомб (0 - без ограничений).
ArchiveMaxFileSize 10M
ArchiveMaxRecursion 5
ArchiveMaxFiles 1000
ArchiveLimitMemoryUsage
```

И далее в файле вы найдете несколько строк для работы с Clamuko. Это интерфейс к модулю Dazuko (http://dazuko.org), обеспечивает (только для Linux) работу clamd в режиме on-access через устройство /dev/dazuko. Это пока еще экспериментальная разработка, пока я не убедился в необходимости пользоваться ею, поэтому, если кто-то заинтересовался, за подробностями обращайтесь в документацию, в ней все понятно расписано.

Запущенный демон ничего не делает. Для указания того, чем именно сейчас ему заниматься, необходимо послать сигнал:

- PING – проверка связи, в ответ демон посылает PONG, и закрывает соединение.
- VERSION – вывод версии.
- RELOAD – перезагрузка антивирусных баз.
- QUIT – остановка демона.
- SCAN file/directory – рекурсивный обход указанных каталогов в поисках вирусов с поддержкой архивов (если не запрещено в конфигурационном файле).
- RAWSCAN file/directory – то же, только без поддержки работы с архивами.
- CONTSCAN file/directory – то же, что и SCAN, но при обнаружении вируса программа не прерывает свою работу, а продолжает обход каталога дальше.
- STREAM – просмотр потока, при этом демон выдаст номер порта, в который необходимо посылать сигнал.

С сигналами понятно, только вот как их посылать, в документации сказано довольно невнятно. Оказалось, все замешано на межпроцессорном взаимодействии или подключении к сетевому порту. Например, команду «просканировать каталог» можно дать таким образом (при сетевом режиме работы демона):

```
# telnet localhost 3310
```

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
CONTSCAN /home/sergej/work
/home/sergej/work/clamav-0.65.tar.gz: ClamAV-Test-Signature FOUND
/home/sergej/work/clamav-0.65/test/test1: ClamAV-Test-Signature FOUND
/home/sergej/work/clamav-0.65/test/test1.bz2: ClamAV-Test-Signature FOUND
/home/sergej/work/clamav-0.65/test/test2.zip: ClamAV-Test-Signature FOUND
/home/sergej/work/clamav-0.65/test/test2.badext: ClamAV-Test-Signature FOUND
Connection closed by foreign host.
```

Поэтому все-таки более удобным способом является использование утилиты clamdscan, просто введя в качестве аргумента проверяемый каталог или файл.

```
#clamdscan /home
```

Для автоматического запуска clamd вместе с системой необходимо положить файл clamd.sh в каталог /etc/init.d/ и прописать путь для запуска в /etc/rc.d/rc.local или создать символическую ссылку в каталоге соответствующему уровню запуска системы.

```
#ln -s /etc/init.d/clamd.sh /etc/rc.d/rc5.d/S50clamd
```

Хотя все в этом вопросе зависит от используемой операционной системы или дистрибутива Linux.

С clamav-milter все просто. Если антивирус устанавливался при помощи rpm-пакетов, то необходимо доустановить пакет clamav-milter-0.65-4.i386.rpm, в котором практически все уже настроено, и в каталоге /usr/share/doc/clamav-milter-0.65/ лежат документы RPM-clamav-milter.txt и HOWTO-logwathch.txt, в которых все расписано по шагам. При установке из исходников также ничего сложного. Добавляем в файл /etc/mail/sendmail.mc строку:

```
INPUT_MAIL_FILTER(`clmilter',`S=local:/var/run/clmilter.sock,
F=, T=S:4m;R:4m')dnl
define(`confINPUT_MAIL_FILTERS', `clmilter')
А в clamav.conf проверяем наличие таких строк.
LocalSocket /var/run/clamd.sock
ScanMail
StreamSaveToDisk
```

И запускаем утилиту:

```
#/usr/local/sbin/clamav-milter -blo /var/run/clmilter.sock
```

При необходимости ограничить число процессов добавляем опцию -max-children=, если clamd работает в сетевом режиме, то дополнительно используется опция -server= с указанием IP-адреса, последним аргументом в этом случае проставляется номер порта.

Утилита автоматического обновления антивирусных баз может запускаться в двух режимах: интерактивном – из командной строки, и как демон. Утилита использует базу http://database.clamav.net для автоматического выбора зеркала. В комплекте имеется также список таких баз, занесенный в файл mirror.txt, утилита пробует по порядку соединиться с первым в списке и в случае неудачи далее следует по списку. Можно подобрать для себя оптимальный вариант и поставить его первым. Для начала следует запустить утилиту без параметров, если все нормально, то следующим создать лог-файлы, необходимые для работы.

```
# touch /var/log/clam-update.log
# chmod 600 /var/log/clam-update.log
# chown clamav /var/log/clam-update.log
```

Для запуска в режиме демона используется опция -d:

```
# freshclam -d -c 3 -l /var/log/clam-update.log
```

Параметр -c указывает на промежуток времени обновления базы в днях (число от 1 до 50). Для указания отличной от установленной по умолчанию директории, в которую должны помещаться обновления, используйте опцию -datadir=. Прокси можно указать двумя способами: либо задать в командной строке параметры -http-proxy=hostname[:port] и при необходимости указания пароля для доступа -proxy-user=user:password; второй вариант – установить нужное значение переменной http_proxy:

```
#export http_proxy="proxy.server:8080"
```

Для контроля за обновлениями можно воспользоваться параметрами: -on-error-execute=COMMAND и -on-update-execute=COMMAND. Первая позволяет задать команду, которая будет выполнена при неудачном обновлении баз, вторая – наоборот, при успешном проведении обновления. Для одноразового запуска утилиты в случае необходимости немедленного обновления она запускается без опции -d (да и -c смысла не имеет). Остальные параметры при этом остаются теми же. В rpm-пакете лежит файл-шаблон /etc/sysconfig/freshclam, в котором можно заполнить соответствующие поля для установки всех вышеперечисленных параметров, а запускать утилиту при помощи скрипта /etc/init.d/freshclam. Можно для запуска использовать и cron, занеся в /etc/crontab для еженедельного обновления примерно такую строку:

```
0 00 * * 07 /usr/local/bin/freshclam --quiet ↵
   -l /var/log/clam-update.log
```

И последняя, довольно интересная утилита sigtool, позволяющая самим создать готовую сигнатуру для добавления в свою антивирусную базу. Таким образом можно попробовать самим создать себе антидот во время очередной эпидемии до реакции компаний, выпускающих антивирусное ПО. Естественно, это все-таки полумера, т.к. автоматически без глубокого анализа будет довольно трудно так сразу создать сигнатуру, действующую на все варианты обнаруженого вируса, особенно в случае полиморфного варианта. В документе «Creating signatures for ClamAV», который поставляется вместе с архивом, расписано, как получить сигнатуру из тестовых «вирусов», поставляемых вместе в ClamAV. Мне повезло чуть больше. Погоняв чуть дольше недели антивирус в боевом режиме, удалось найти вирус который ClamAV не обнаружил, а Dr.Web по его поводу сказал следующее:

```
#drweb   /mnt/dos.ext.1/virus_test/
```

```
Dr.Web (R) for FreeBSD, version 4.30 (October 7, 2003)
Report dated 24 January 2004, 15:09:37
Command line: -path=/mnt/dos.ext.1/virus_test/
Key file: /usr/local/drweb/drweb.key
Registration info:
0100000004
Evaluation key ID Anti-virus Lab St.Petersburg
This is an EVALUATION version with limited functionality!
To get your registration key, call regional dealer.
Loading /var/drweb/bases/drw43009.vdb - Ok, virus records: 115
...
Loading /var/drweb/bases/drwebase.vdb - Ok, virus records: 39721
Total virus records: 41300
/mnt/dos.ext.1/virus_test/test.exe infected with Win32.HLLP.Underscore.36864
/mnt/dos.ext.1/virus_test/test.zip - archive ZIP
Scan report for "/mnt/dos.ext.1/virus_test/":
Scanned      : 1        Cured     : 0
Infected     : 1        Deleted   : 0
Modifications : 0       Renamed   : 0
Suspicious   : 0        Moved     : 0
Scan time    : 00:00:01  Scan speed : 1087 Kb/s
```

Другой антивирус F-prot, о котором речь пойдет в следующий раз, выдал сообщение:

```
Infection: W32/Underscore.A
```

Очевидно, разработчики ориентируются в первую очередь на новые, недавно появившееся вирусы, и антивирус пока плохо знаком со старой гвардией. Сначала попробуем создать такую сигнатуру при помощи clamscan:

```
# sigtool -c "clamscan --stdout" ↵
   -f   /home/sergej/virus_test/test.exe -s
```

```
"Win32.HLLP.Underscore.36864"
ERROR: String  Win32.HLLP.Underscore.36864 not found in scanner's output.
Please check it and try again.
Does the scanner write to stdout ? It has to.
```

Опция -c говорит, какую команду запускать, здесь должен быть один из установленных в системе антивирусов, -f задает инфицированный файл, а -s – уникальная строка, которую вывел антивирус, обнаруживший вирус, в большинстве случаев сюда пишем имя обнаруженного вируса. Как видите, при помощи clamscan обнаружить его не получилось, поэтому пробуем Dr.Web.

```
# sigtool -c "drweb" -f  -f  /home/sergej/virus_test/test.exe ↵
   -s  "Win32.HLLP.Underscore.36864"
```

```
Detected, decreasing end 1113799 -> 891039
...
Detected, decreasing end 445519 -> 222759
Not detected at 0, moving forward.
Detected, decreasing end 111380 -> 0
Not detected at 0, moving forward.
...
Not detected, moving backward 27866 -> 27816
ERROR: Generated signature is too big.
```

То есть сигнатура получилась больше, чем рекомендуемые 40... 200 символов. В этом случае в документе показано, как вручную найти нужную сигнатуру, но для этого как минимум необходимо немного знать что-то о виру-

се. Этот вирус, например, переименовывает файлы и создает в системном каталоге файл mc42.exe. Поэтому при помощи Midnight Commander, или дав такую команду:

```
# strings test.exe | less
```

или двоичный дамп для анализа:

```
#cat  test.exe  | sigtool --hex-dump > virus.sig
```

а лучше, воспользовавшись двоичным редактором, находим специфические для данного вируса строки (рис. 1) и заносим их в отдельный файл. Но этот метод хоть интересен и работает на ура, мне созданная таким образом сигнатура позволила найти все файлы на зараженном компакте, в том числе и упрятанные в архив (куда не смог заглянуть Dr.Web), но все-таки этот процесс может занять значительный промежуток времени, особенно при большом исходном файле. Можно попробовать разбить исходный файл на меньшие по размеру, в котором(ых) внешний антивирус будет еще находить вирус, и затем повторить операцию. Разбить файл на части можно, воспользовавшись, например, split. Мне удалось, немного повозившись, создать такой файл в 10 Кб и в результате:

```
# sigtool -c "drweb" -f  -f  /home/sergej/work/xaf ↵
    -s  "Win32.HLLP.Underscore.36864"
```

```
The scanner was executed 26 times.
The signature length is 54 (108 hex)
Saving signature in /home/sergej/work/xaf.sig file.
Saving binary signature in /home/sergej/work/xaf.bsig file.
```

В результате в файле xaf.sig будет примерно такая строка.

```
433A5C57494E444F57530000433A5C00583A0000770000007200000534F46545741
52 455C4D6963726F66745C576E5C52756E0000005C0000006D6334322E658650000
```

Добавляем в ее начало:

```
Win32.HLLP.Underscore.36864  (Clam)=
```

Теперь осталось добавить сигнатуру вируса в базу данных.

Распаковываем одну из установленных баз, их имеется две – main.cvd и daily.cvd. Первая – постоянная, вторая – для ежедневных обновлений. Распаковываем нужную:

```
#sigtool  --unpack-current  daily.cvd
```

после чего в текущем каталоге появится файл viruses.db2, если его открыть в любимом редакторе, то увидим, что он состоит из подобных строк. Добавляем в него сигнатуру и просчитываем новую контрольную сумму:

```
#cat  xaf.sig  >> viruses.db2
#md5sum viruses.db2 > viruses.md5
```

Теперь можно пользоваться обновленной базой, указав на нее параметром -d или поместив обратно в каталог /var/lib/clamav или /usr/local/share/clamav/ к старым базам, после чего добавленный таким образом вирус будет обнаруживаться ClamAV. К сожалению, антивирусные компании не очень любят делиться своими наработками, поэтому как-то приделать внешние базы пока не получается, но некоторые сигнатуры в удобочитаемом виде можно взять, например, на Sophos http://www.us.sophos.com/downloads/ide/, по крайней мере Bagle появился там быстро, а простота операции позволила также оперативно занести информацию о нем в свою базу. В документации показано, как можно затем обратно упаковать базу, воспользовавшись опцией --build, но для этого необходимо иметь доступ к специальному серверу, для подписи, поэтому дальше я не пошел, оставил все как есть.

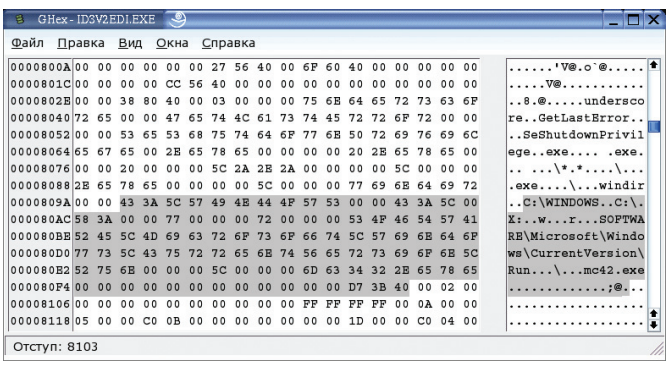


Рисунок 1

Предвидя некоторую критику, сразу отвечу: да, не дело сисадмина собирать по всему свету сигнатуры. Но, с другой стороны, так можно среагировать все-таки побыстрее, чем антивирусные компании (ну, по крайней мере, такая возможность греет душу), плюс новые сигнатуры добавляются в базу данных ClamAV ежедневно, поэтому, я думаю, эта проблема будет решена в скором времени. Мне этот антивирус в общем-то понравился и не в последнюю очередь разнообразием инструментов и удобством работы. Также одним из положительных моментов знакомства с ним отмечаю именно открытость продукта, позволившую наконец разобраться с технологией и понять реальный механизм работы антивирусов. Для сомневающихся в следующих статьях продолжим поиск. Успехов!