Dr.WEB®
Антивирус

Защити созданное

Инструкции по обновлению антивирусного ядра до версии 5.0

«Выпуск новой версии для компании «Доктор Веб», которая предельно ответственно относится к смене цифры версии, — это всегда большой шаг вперед в разработке. Учитывая масштабы и сложность современных угроз, мы сосредоточили свои усилия на новейших технологиях защиты, которые позволяют нам не только эффективно отражать атаки известных вирусов, но и быть готовыми защитить пользователей от новых, еще неизвестных вредоносных программ»

**Игорь Данилов, автор антивируса Dr.Web,
технический директор компании «Доктор Веб»**

125124, Россия, Москва,
3-я улица Ямского поля,
вл.2, корп. 12а

Телефон:
+7 (495) 789-45-87
(многоканальный)

Факс:
+7 (495) 789-45-97

www.drweb.com
www.freedrweb.com
www.av-desk.com

В конце 2008 года компания «Доктор Веб» заявила о значительном шаге в развитии антивирусных решений семейства Dr.Web, выпустив новую версию «Антивируса Dr.Web для Windows» под номером 5.0, которая дала старт обновлению всей линейки продуктов компании.

Модернизированные продукты помимо множества новых модулей используют обновленное и усовершенствованное антивирусное ядро.

Назначение документа

Данный документ предназначен для использования в компаниях и организациях, уже внедривших решения Dr.Web для операционных систем типа Unix (Linux, FreeBSD, Solaris) версий 4.44 либо реализовавших на их основе свои продукты и не желающих переходить на новые версии в связи с наличием риска приостановки бизнес-процессов на период миграции, необходимостью изучения документации на новые, зачастую значительно переработанные, продукты. Однако использование устаревших версий повышает риск проникновения вредоносных объектов через защищаемый периметр локальной сети, так как для поддержания достаточного уровня информационной безопасности необходимо не только проводить обновления антивирусных баз, но и обновлять само антивирусное ядро, обеспечивающее обнаружение вредоносных объектов новейшего типа.

Описанная ниже процедура позволяет провести обновление антивирусного ядра практически на лету - без полной замены и настройки установленного антивирусного программного обеспечения.

Антивирусное ядро 5.0

Совершенствование технологий несигнатурного поиска

Наряду с традиционным сигнатурным поиском вредоносных программ, антивирусные решения Dr.Web используют интеллектуальный эвристический анализатор и уникальную технологию Origins Tracing .

В новую версию антивирусного ядра вошли последние наработки специалистов компании «Доктор Веб» по улучшению этих технологий. Акцент на развитие возможностей несигнатурного поиска позволяет антивирусным решениям Dr.Web постоянно повышать уровень превентивной защиты, оберегающей персональные компьютеры, серверы и устройства пользователей от неизвестных угроз, количество которых с каждым днем только увеличивается.

Работа с архивами и упаковщиками

Антивирусные решения Dr.Web поддерживают проверку большинства существующих форматов упакованных файлов и архивов с любой степенью вложенности, в том числе, проверку многотомных и самораспаковывающихся архивов. Так, например, Dr.Web может работать с более чем 1000 видов упаковщиков и различных видов архивов, некоторые из которых не известны ни одной другой антивирусной программе.

В версии 5.0 была введена поддержка новых упаковщиков и архивов (PDF, AutoIt, AScript, EncryptPE, Thinstall, RSFX и т.д.), а так же исправлены неточности в работе предыдущих версий антивирусного ядра (например, при работе с архивами 7ZIP, BZIP2, ZLIB, AR).

Однако самым главным нововведением в области анализа упакованных файлов в версии 5.0 стало введение новой, уникальной технологии FLY-CODE™, универсального распаковщика.

Универсальный распаковщик FLY-CODE™

Технология FLY-CODE на данный момент не имеет аналогов у других разработчиков антивирусных средств. Предложенный специально для антивирусного ядра 5.0 универсальный алгоритм распаковки позволяет строить эвристические предположения о наличии вредоносных объектов в файлах, сжатых не только известными антивирусу Dr.Web упаковщиками, но и новыми, ранее неисследованными программами.

К названиям вредоносных объектов, обнаруженные с использованием новой технологии, добавляется суффикс «Trojan.Packed».

Быстродействие

Антивирусные решения Dr.Web всегда славились низкими системными требованиями и высокими скоростями проверки, тем не менее, путем оптимизации антивирусного ядра в версии 5.0 специалистам компании «Доктор Веб» удалось достичь ускорения процесса проверки еще на 30% по сравнению с предыдущей версией.

Прочее

Версия 5.0 так же включает в себя исправления ряда недостатков и проблем предыдущей версии. Так, например, в новом ядре ликвидированы причины падений антивируса при анализе некоторых DOS-файлов, RAR-архивов и поврежденных OLE-объектов, а так же исправлены обнаруженные ошибки, ведущие к зависанию система, а так же проблемы при лечении макровирусов в текстовых файлах.

Обновление ядра для UNIX®-подобных систем

Антивирусное ядро Dr.Web не зависит от типа и версии операционной системы и может применяться свободно как на компьютерах, работающих под управлением операционных систем семейства Microsoft® Windows®, так и в UNIX®-подобных системах (например, Linux®, FreeBSD® и т.д.).

Программный интерфейс (API) антивирусного ядра Dr.Web версии 5.0 остался прежним по сравнению с версией 4.44, поэтому в рамках антивирусных решений для UNIX-подобных систем возможен упрощенный переход на использование новой версии – усовершенствованное ядро полностью совместимо со всеми компонентами программных комплексов версии 4.44.

Обновляемые компоненты

Для обновления установленного антивирусного ядра необходимо заменить файлы, входящие в состав пакета `drweb-bases – drweb32.dll`, `update.drl`, антивирусные базы, находящиеся в каталоге `/var/drweb/bases/`

Внимание! Размещение файла `drweb32.dll` зависит от типа операционной системы:

`/opt/drweb/lib/drweb32.dll` - для операционных систем Linux и Solaris

`/usr/local/drweb/lib/drweb32.dll` - для FreeBSD

После обновления ядра и вирусных баз для защиты вашей системы будут применяться все усовершенствования, реализованные в антивирусном ядре Dr.Web версии 5.0.

Процедура обновления

Внимание! Для осуществления процедуры установки антивирусного ядра необходимы права администратора (`root`).

Обновление антивирусного ядра до версии 5.0. может быть выполнено в полуавтоматическом режиме:

1. Создать резервную копию имеющихся файлов. Например, переименовав или скопировав их в отдельную директорию:

   ```
   # cd /var/drweb/bases/
   # cp update.drl update.drl.444
   ```

2. Загрузить файл `update.drl`

   Например:

   ```
   # cd /tmp/
   # wget ftp://ftp.drweb.com/pub/drweb/unix/misc/update.drl
   ```

3. Заменить ранее установленные файл:

   ```
   # cp /tmp/update.drl /var/drweb/bases/
   ```

4. Изменить права доступа:

   Например, для операционных систем Linux, Solaris:

   ```
   # chown -R drweb:drweb /{opt,var}/drweb/
   ```

5. Обновить базы до версии 5.0 с помощью скрипта обновления `update.pl`:

   Например:

   для операционных систем Linux, Solaris:

   ```
   # su –m drweb –c /opt/drweb/update.pl
   ```

   для операционных систем семейства FreeBSD:

   ```
   # su –m drweb –c /usr/local/drweb/update.pl
   ```

   Внимание! В связи с особенностями работы команды su после ввода этой команды может появиться сообщение типа "`bash: /root/.bashrc: Permission denied`". Наличие данного сообщения не является препятствием для выполнения обновления

   Корректность проведенного обновления можно проверить по сообщениям в системных логах или по сообщениям при перезапуске антивирусного демона

   ```
   # /etc/init.d/drwebd restart
   ```

```
Loading /var/drweb/bases/drwtoday.vdb - Ok, virus records: 125
Loading /var/drweb/bases/drw50029.vdb - Ok, virus records: 2691
Loading /var/drweb/bases/drw50028.vdb - Ok, virus records: 3327
Loading /var/drweb/bases/drw50027.vdb - Ok, virus records: 4697
Loading /var/drweb/bases/drw50026.vdb - Ok, virus records: 2792
Loading /var/drweb/bases/drw50025.vdb - Ok, virus records: 5841
Loading /var/drweb/bases/drw50024.vdb - Ok, virus records: 2260
Loading /var/drweb/bases/drw50023.vdb - Ok, virus records: 4796
Loading /var/drweb/bases/drw50022.vdb - Ok, virus records: 5098
Loading /var/drweb/bases/drw50021.vdb - Ok, virus records: 4891
Loading /var/drweb/bases/drw50020.vdb - Ok, virus records: 5033
Loading /var/drweb/bases/drw50019.vdb - Ok, virus records: 3254
Loading /var/drweb/bases/drw50018.vdb - Ok, virus records: 5241
Loading /var/drweb/bases/drw50017.vdb - Ok, virus records: 7585
Loading /var/drweb/bases/drw50016.vdb - Ok, virus records: 5298
Loading /var/drweb/bases/drw50015.vdb - Ok, virus records: 5947
Loading /var/drweb/bases/drw50014.vdb - Ok, virus records: 6039
Loading /var/drweb/bases/drw50013.vdb - Ok, virus records: 5309
Loading /var/drweb/bases/drw50012.vdb - Ok, virus records: 3511
Loading /var/drweb/bases/drw50011.vdb - Ok, virus records: 2495
Loading /var/drweb/bases/drw50010.vdb - Ok, virus records: 4565
Loading /var/drweb/bases/drw50009.vdb - Ok, virus records: 4467
Loading /var/drweb/bases/drw50008.vdb - Ok, virus records: 5196
Loading /var/drweb/bases/drw50007.vdb - Ok, virus records: 2359
Loading /var/drweb/bases/drw50006.vdb - Ok, virus records: 1938
Loading /var/drweb/bases/drw50005.vdb - Ok, virus records: 3335
Loading /var/drweb/bases/drw50004.vdb - Ok, virus records: 3185
Loading /var/drweb/bases/drw50003.vdb - Ok, virus records: 1468
Loading /var/drweb/bases/drw50002.vdb - Ok, virus records: 280
Loading /var/drweb/bases/drw50001.vdb - Ok, virus records: 567
Loading /var/drweb/bases/drw50000.vdb - Ok, virus records: 1194
Loading /var/drweb/bases/drwebase.vdb - Ok, virus records: 423328
Loading /var/drweb/bases/dwrtoday.vdb - Ok, virus records: 491
Loading /var/drweb/bases/dwr50001.vdb - Ok, virus records: 626
Loading /var/drweb/bases/dwntoday.vdb - Ok, virus records: 478
Loading /var/drweb/bases/dwn50002.vdb - Ok, virus records: 925
Loading /var/drweb/bases/dwn50001.vdb - Ok, virus records: 840
Loading /var/drweb/bases/drwrisky.vdb - Ok, virus records: 3316
Loading /var/drweb/bases/drwnasty.vdb - Ok, virus records: 19303
Total virus records: 564091
Key file: /opt/drweb/drweb32.key - loaded.
License key number: 0010745318
```

Подтверждением корректности проведенного обновления является строка "`Engine version: 5.0.0.XXXXX`", а также загрузка баз с именами типа `drw50xxx.vdb`

В том случае, если обновление прошло неудачно, то для восстановления работоспособности ранее использовавшейся версии необходимо выполнить команды:

`# cd /var/drweb/bases/`

`# mv update.drl.444 update.drl`

`# su -m drweb -c /opt/drweb/update.pl` (Linux, Solaris)

125124, Россия, Москва, 3-я улица Ямского поля, вл.2, корп. 12а
Телефон: +7 (495) 789-45-87 (многоканальный)
Факс: +7 (495) 789-45-97

www.drweb.com
www.freedrweb.com
www.av-desk.com