Антивирус DR.Web

Группа 2СА-1

Выполнил Филатов Д.А.

Dr.Web

- **Dr.Web** — общее название семейства антивирусного ПО для различных платформ (Windows, macOS, Linux, мобильные платформы) и линейки программно-аппаратных решений (Dr.Web Office Shield), а также решений для обеспечения безопасности всех узлов корпоративной сети (Dr.Web Enterprise Suite). Разрабатывается компанией «Доктор Веб».
- Продукты предоставляют защиту от вирусов, троянского, шпионского и рекламного ПО, червей, руткитов, хакерских утилит, программ-шуток, а также неизвестных угроз с помощью различных технологий реального времени и поведенческого анализа

Особенности

- Возможность установки на зараженную машину.
- Обнаружение и лечение сложных полиморфных, шифрованных вирусов и руткитов.
- Возможность настройки копирования важных данных в защищённое хранилище позволяет пользователям версии Dr.Web для Windows самостоятельно восстанавливать поврежденные данные без необходимости обращения в службу технической поддержки «Доктор Веб».
- Поддержка большинства существующих форматов упакованных файлов и архивов, в том числе многотомных и самораспаковывающихся архивов.
- Компактная вирусная база и небольшой размер обновлений. Одна запись в вирусной базе позволяет определять до тысячи подобных вирусов.
- Обновления вирусных баз производятся немедленно по мере выявления новых вирусов, до нескольких раз в час. Разработчики антивирусного продукта отказались от выпуска обновлений вирусных баз по какому-либо графику, поскольку вирусные эпидемии не подчиняются таковым.
- Кроссплатформенность — используется единая вирусная база и единое ядро антивирусного сканера на разных платформах ОС.
- Низкое влияние на производительность системы. Благодаря технологиям оптимизации, заведомо чистые файлы не проверяются компонентами Dr.Web, что снижает нагрузку на систему.

История создания

История разработки антивируса Игоря Данилова начинается с 1991 года, а под маркой Dr.Web антивирусы разрабатываются и распространяются с 1994 года.

- 1992 год — создание первой версии антивирусной программы Spider’s Web (прототипа Dr.Web). В ней была реализована идея выполнения кода программ в эмуляторе процессора для поиска неизвестных вирусов.
- 1993 год — участие программы Spider’s Web на международной выставке CeBIT.
- 1994 год — начало продаж антивируса Doctor Web, призванный заменить популярную в то время в России антивирусную программу Aidstest, которая не могла бороться с появившимися полиморфными вирусами, полностью изменяющими свой код при каждом заражении.
- 1995 год — демонстрация Антивирусного комплекта DSAV 2.0. В комплект входит антивирус Doctor Web.
- 1996 год — дебют программы Dr.Web (версия 3.06b) на сравнительном тестировании полифагов, проводимом журналом Virus Bulletin, более чем впечатляющий — как по уровню знания полиморфных вирусов, так и по качеству эвристического анализатора. В статье журнала Virus Bulletin о программе Doctor Web (версия 3.08) был особо отмечен эвристический анализатор антивируса, который в режиме «параноик» определил 100 % полиморфных вирусов. Представлена альфа-версия Dr.Web для Novell NetWare.
- 1997 год — впервые российская антивирусная программа (Dr.Web) вошла в тройку лучших антивирусов мира по результатам тестирования журнала Virus Bulletin. Выходит бета-версия Dr.Web для Novell NetWare.
- 1998 год — выход Dr.Web 4.0. Изменена архитектура и алгоритм работы программы. Публичное тестирование Dr.Web для Windows 95/98/NT.
- 1999 год — появление резидентного модуля SpIDer Guard для Windows 95/98. Dr.Web для Windows 95/98/NT получает первую награду VB100 в тестах журнала Virus Bulletin. Выход коммерческой версии Dr.Web для Windows 95/98/NT. В Dr.Web впервые реализована проверка памяти виртуальных машин в среде Windows NT.

- 2000 год — Dr.Web получил сертификат соответствия Минобороны России. Резко увеличена частота выхода обновлений вирусной базы — до нескольких раз в час.
- 2001 год — заключено соглашение с компанией Яндекс. С этого момента все письма, проходящие через почтовую систему Яндекс, проверяются с помощью решений Dr.Web.
- 2002 год — создание антивирусных фильтров Dr.Web для почтовых серверов CommuniGate Pro. Выпуск первой бета-версии Dr.Web для Unix с уникальной на тот момент функцией — лечением файлов налету. Выпуск программы SpIDer Mail — уникальной на тот момент программы для проверки входящей почты.
- 2007 год — создание технологии несигнатурного обнаружения вредоносных программ Origins.Tracing.
- 2007 год — открыто публичное тестирование сервиса Dr.Web AV-Desk, на базе которого интернет-провайдеры предоставляют своим абонентам услугу «Антивирус Dr.Web» (первая в российской сфере интернет-бизнеса SaaS-модель).
- 2008 год — появление антивирусного пакета Dr.Web Security Space. Впервые реализован новый компонент для проверки HTTP-трафика — Dr.Web SpIDer Gate.
- 2009 год — начало бета-тестирования антивирусного продукта Dr.Web Security Space Pro Отличается от Dr.Web Security Space наличием сетевого экрана.
- 2010 год — выпуск первого в России антивируса под ОС Android — Dr.Web для Android.
- 2013 год — выпуск нового продукта Dr.Web Security Space 9. Новые функции Dr.Web Cloud, превентивная защита, поведенческий анализатор Dr.Web Process Heuristic, защита пользовательских данных от повреждения, комплексный анализатор упакованных угроз, проверка трафика по всем протоколам, функция «Безопасный поиск», защита общения в популярных сервисах мгновенных сообщений и другие функции.
- 2014 год — выпуск 10 версии антивируса.
- В сентябре 2015 года на Украине продукты компании попали под запрет государственных закупок товаров и услуг. Некоторые СМИ ошибочно сообщили, что «санкции предусматривают блокировку активов и приостановление выполнения экономических и финансовых обязательств со стороны Украины».
- 2015 год — в ноябре вышел Dr.Web Security Space 11, основными нововведениями которого стало усиление самозащиты и превентивной защиты, в частности, новая технология Dr.Web ShellGuard позволила обеспечить защиту от эксплойтов, использующих т. н. уязвимости «нулевого дня».
- 2015 год — выпуск продукта Dr.Web Katana (технологии которого входит в состав Dr.Web Security Space), решения для защиты, которое сочетается с уже установленным антивирусом другого производителя.
- 2016 год — выпуск продукта Dr.Web Katana Business Edition. Внесение продуктов Dr.Web в Единый реестр отечественного ПО. Dr.Web Enterprise Security Suite версии 10.0 сертифицирован ФСТЭК России.

Продукты

- CureIt!
- CureNet!
- Dr.Web vxCube
- Dr.Web Mobile Security Suite

CureIt!

- Dr.Web CureIt! — утилита для проверки и лечения зараженных рабочих станций на платформе Windows от вредоносного ПО. С версии 8.0 используется универсальная подсистема нейтрализации угроз Anti-rootkit API (ArkAPI), что позволяет лечить систему от вредоносного ПО любой сложности. Оснащен интуитивно понятным интерфейсом, благодаря которому пользователь может в несколько кликов проверить и, в случае заражения, вылечить свой ПК. Для опытных же пользователей есть выборочная проверка. Оснащен собственным менеджером карантина, что позволяет восстанавливать резервные копии вылеченных/удаленных файлов даже при повторном запуске утилиты. Используется тот же файловый движок, что и в антивирусе.
- Число запусков данной программы не ограничивается. Для обновления антивирусной базы необходимо загрузить с сайта актуальную версию программы (нет возможности автоматического обновления).
- С осени 2009 года изменены условия лицензирования сканера — теперь бесплатно использовать его могут только домашние пользователи, использование для организаций и в коммерческих целях стало платным. Кроме того, пользователь бесплатной утилиты обязуется участвовать в программе улучшения качества программного обеспечения, для чего информация, собранная во время проверки компьютера, автоматически отправляется в компанию «Доктор Веб».

CureNet!

- Dr.Web CureNet! — сетевая утилита с централизованным управлением для удаленной проверки и лечения зараженных рабочих станций и серверов Windows даже полностью изолированных от Интернета. Позволяет использовать одновременно 2 антивируса на рабочих станциях и файловых серверах Windows: Dr.Web и антивирус другого производителя.

Dr.Web vxCube

- Сервис экстренного анализа вредоносных и потенциально вредоносных файлов. Dr.Web vxCube позволяет не только проанализировать файл, но и получить специальную сборку лечащей утилиты Dr.Web CureIt!, в которую включен механизм обезвреживания анализируемого объекта. Схема работы Dr.Web vxCube проста: пользователь получает доступ для отправки подозрительных файлов на «облачный» анализ, анализатор запускает отправленный объект и изучает его поведение, после чего выносит вердикт. Сервис позволяет максимально быстро обезвредить новейшую угрозу, не дожидаясь обновлений используемых средств защиты. Проверка отправленных файлов занимает в среднем не более минуты, будь то исполняемые файлы Windows, офисные документы или скрипт-файлы. Проверяемый объект запускается на исполнение на виртуальной машине, при этом клиент сервиса может удаленно — через интерфейс Dr.Web vxCube — наблюдать за ходом анализа. Технический отчет о результатах исследования включает видеозапись работы анализатора. Также можно получить полный отчет о том, как именно исследуемая программа действует в системе, какие вносит в неё изменения, с какими ресурсами соединяется, а также увидеть карту сетевой активности этой программы и многое другое.

Dr.Web Mobile Security Suite

- Это программное обеспечение, предназначенное для комплексной защиты мобильных устройств. В Dr.Web Mobile Security Suite объединены средства защиты для мобильных устройств под управлением Windows Mobile, Symbian OS, BlackBerr OS и Android. Разработчики компании реализовали технологию фильтрации входящих телефонных звонков и СМС-сообщений на основе чёрного и белого списков. Для платформы Android существует бесплатная версия Антивирус Dr.Web Light, в которой нет модуля фильтрации звонков и SMS-сообщений, а также отсутствует компонент «Антивор». На данный момент Антивирус Dr.Web Light занимает первое место в поиске антивирусов в Google Play в России.

Список литературы

https://ru.wikipedia.org/wiki/Dr.Web