УДК 004.491.22

Устройство антивирусов на примере KAV

Карташов А.А. 11-В

Актуальность: Антивирусы применяются для каждой ОС, защищая её от вредоносных и неблагоприятных объектов. Антивирусы, использующие метод обнаружения подозрительного поведения программ не пытаются идентифицировать известные вирусы, вместо этого они прослеживают поведение всех программ. Если программа пытается выполнить какие-либо подозрительные с точки зрения антивирусной программы действия, то такая активность будет заблокирована, или же антивирус может предупредить пользователя о потенциально опасных действиях такой программы.

Цель: Полностью раскрыть данную тему, проанализировать её, сделать выводы.

Антивирусная программа (антивирус) —программа для обнаружения и лечения вредоносных объектов или инфицированных файлов, а также для профилактики — предотвращения заражения файла или операционной системы вредоносным кодом.

Существует несколько основных методов поиска вирусов, которые применяются антивирусными программами: сканирование; эвристический анализ; обнаружение изменений; резидентные мониторы.

Конструктивная особенность антивируса:

1. Ядро
2. Сканер
3. Монитор активности
4. Модуль обновления
5. Модуль контроля скриптов и модули контроля трафика

Наличие 5 пункта не всегда соблюдается. Весь потенциал антивирусов заложено в ядро, которое отвечает за проверку файлов, это сердце программы, которое и отвечает за работу всей программы в общем. Именно

ядро отвечает за проверку хранящейся на компьютере информации, а так же определением вредоностных программ. От того, какие методы были реализованы для поиска и определения вирусов, зависит функциональность антивируса, в общем. Основным методом обнаружения вредоносного кода у большинства антивирусов, является сигнатурный анализ (выявление вирусов по их цифровому «отпечатку» или сигнатуре).

Важнейшие характеристики такого анализа – это скорость и количество системных ресурсов, затраченных на его проведение, а так же количество ложных обнаружений вирусов. Немалую роль в этом играет размер и полнота сигнатур, а так же технологии их создания и использования. Чем больше сигнатура, тем обычно меньше вероятность ложного обнаружения и выше достоверность определения вирусов. Вместе с тем увеличивается также потребность в вычислительных ресурсах, необходимых ядру для проверки. Минусом этого метода является низкая эффективность при обнаружении новых вирусов, а также модификаций известных уже вирусов, и, как следствие, снижение эффективности защиты в целом. Так же большим недостатком сигнатурного метода обнаружения вирусов является большой разрыв по времени между появлением первых случаев заражения и появления метода их лечения. Но по исследованиям крупных антивирусных компаний стало ясно, что это самый надежный способ, т.к. он составляет около 30% эффективности от всех методов антивируса.

Антивирусное ядро — реализация механизма сигнатурного сканирования и эвристического анализа на основе имеющихся сигнатур вирусов.

Антивирусный комплекс — набор антивирусов, использующих одинаковое антивирусное ядро или ядра, предназначенный для решения практических проблем по обеспечению антивирусной безопасности компьютерных систем. В антивирусный комплекс также в обязательном порядке входят средства обновления антивирусных баз.

Помимо этого антивирусный комплекс дополнительно может включать в себя поведенческие анализаторы и ревизоры изменений, которые вовсе не используют антивирусное ядро.

В качестве примера рассмотрим антивирус Касперского:

Антивирус Касперского (англ. Kaspersky Antivirus, KAV) — антивирусное программное обеспечение, разрабатываемое Лабораторией Касперского. Предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, руткитов, adware, а также неизвестных угроз с помощью проактивной защиты, включающей компонент HIPS. Первоначально, в начале 1990-х, именовался -V, затем — AntiViral Toolkit Pro.

К основным функциям антивируса Касперского относятся: базовая защита, предотвращение угроз, восстановление системы и данных, защита конфиденциальных данных и удобство использования. Рассмотрим каждую из этих функций подробнее.

Базовая защита проверяет файлы в автоматическом режиме и по требованию, а так же интернет-трафик (для любых интернет-браузеров),защищает от вирусов, троянских программ, червей, шпионских и рекламных программ. Используется проактивная защита от новых вредоносных программ и Интернет - пейджеров (ICQ, MSN).

Предотвращение угроз включает в себя поиск уязвимостей в ОС и установленном ПО, анализ и устранение уязвимостей в браузере Internet Explore , распознавание вирусов по способу их упаковки и глобальный мониторинг угроз (Kaspersky Security Network).

Восстановление системы и данных даёт возможность установки программы на зараженный компьютер, защищает программы от выключения или остановки, а так же восстанавливает корректные настройки системы после удаления вредоносного ПО.

Защита конфиденциальных данных блокирует ссылки на фишинговые сайты, защищает от всех видов кейлоггеров.

Удобство использования заключается в автоматической настройке программы в процессе установки, в наглядном отображении результатов работы программы и готовые решения (для типичных проблем).

Вывод: Несмотря на широкую распространенность антивирусных программ, продолжают появляться новые вирусы. Чтобы справиться с ними, необходимо создавать более универсальные и качественно-новые антивирусные программы, которые будут включать в себя все положительные качества своих предшественников. К сожалению, на данный момент нет такой антивирусной программы, которая гарантировала бы защиту от всех разновидностей вирусов на 100%.

Список литературы:

1.Антивирусный комплекс [Электронный ресурс] : (с изм. и доп.) – Режим доступа: http://www.sibirity.com/antiviruses/101-2009-02-09-11-5910.html (дата обращения 15.11.2009)

2.Антивирус Касперского [Электронный ресурс] : (с изм. и доп.) – Режим доступа: http://ru.wikipedia.org/wiki/Антивирус_Касперского (дата обращения 10.11.2009)

3. Конструктивная особенность антивируса [Электронный ресурс] : (с изм. и доп.) – Режим доступа: http://unlimmb.info/brain.html (дата обращения 14.11.2009)