Антивирусная защита: новый этап

13.02.2012 Владимир Безмалый

- Ключевые слова :
- Лаборатория
- Антивирусы
- Владимир Безмалый

Средства защиты, не использующие «облачные» технологии, сегодня уже не актуальны. Однако следует понимать, что сегодня производители антивирусного программного обеспечения не в состоянии перенести всю защиту в «облако», так как существует огромное количество угроз не только из Интернета. Реально работающим может быть лишь решение, сочетающее в себе мощную клиентскую составляющую с устойчивой «облачной» службой

Скорость разработки новых вредоносных программ просто поражает: ежедневно появляется примерно 35 тыс. экземпляров. Имеющихся на сегодня в арсенале обычных антивирусов технологий защиты (сигнатурный анализ и проактивная защита) явно недостаточно. Ведь такими темпами в скором времени все ресурсы компьютера будут расходоваться исключительно на обеспечение его защиты.
По данным специалистов «Лаборатории Касперского», в 2007 году количество вредоносного ПО составляло менее 5 млн экземпляров, а в 2009-м мы имеем уже почти 20 млн. Естественно, это привело к существенному увеличению объема антивирусных обновлений, что создает большие неудобства для пользователей.
Таким образом, становится ясно, что традиционные технологии антивирусной защиты (сигнатурный анализ и проактивная защита) уже не в состоянии справляться с возросшим вирусным потоком. Тем более что проактивная защита, всегда применявшаяся как первый эшелон обороны в борьбе с незнакомыми вирусами, не в состоянии отследить более 50–70% вирусов.
Объем антивирусных обновлений в 2007 году, по данным «Лаборатории Касперского», составлял порядка 15 Мбайт за год, в 2010 году этот показатель увеличился до 130 Мбайт.
Дальнейшее принципиальное увеличение максимальной скорости реакции на угрозы с помощью обычных антивирусных обновлений невозможно, так как

затраты времени на обнаружение «вредителей», их последующий анализ и тестирование формируемых антивирусных обновлений уже сведены к минимуму. Таким образом, перед разработчиками антивирусов все чаще встают следующие вопросы:

- Как автоматизировать процессы защиты?
- Как свести размеры баз антивирусных сигнатур к минимуму, сохранив высокий уровень защищенности?
- Как увеличить скорость реакции на появление вредоносного ПО?

Сделать это традиционными средствами уже весьма сложно, практически почти невозможно.

Решение проблемы в «облаках»?

Одним из вариантов решения является создание «облачной» защиты. В продуктах «Лаборатории Касперского» такая защита функционирует с 2008 года в виде Kaspersky Security Network (KSN). KSN собирает и отправляет на серверы «Лаборатории Касперского» информацию обо всех попытках заражения и случаях подозрительного поведения на миллионах пользовательских машин, защищенных продуктами «Лаборатории Касперского», осуществляя постоянный мониторинг вирусной ситуации во Всемирной паутине (см. экран). Таким образом, стоит новой вредоносной программе попытаться заразить лишь один компьютер, как информация о ней и ее действиях попадает к экспертам «Лаборатории Касперского» через Kaspersky Security Network. Система немедленно вырабатывает соответствующие средства защиты (сигнатуры, шаблоны нежелательного поведения, списки адресов вредоносных сайтов) и доставляет их всем пользователям «Лаборатории Касперского». В результате пользователь всегда располагает самой актуальной защитой от новых угроз, поступившей из «облака», независимо от графика регулярного обновления антивирусных баз.

Экран. Окно KSN

Преимущества использования «облачной» технологии антивирусной защиты очевидны:

- высокая скорость реакции на угрозы, вплоть до десятков секунд;
- обладая практически неограниченными вычислительными ресурсами, «облако» позволяет производить параллельную обработку данных, то есть быстро выполнять исследование сложных угроз;
- при работе с «облаком» загрузка пользовательского компьютера минимальна, так как обмен информации с ним, как правило, осуществляется в фоновом режиме.

Как это работает?

Давайте рассмотрим, как работает «облачная» защита, на простом примере. Многие пользователи используют одни и те же программы: браузеры, интернет-пейджеры, утилиты для редактирования изображений и т. д. Данное программное обеспечение регулярно обновляется, при этом сами пользователи или вообще не знают об этом или знают очень и очень мало, ведь часть подобного программного обеспечения (например, от компании Adobe, Google и т. д.) обновляется вообще без ведома пользователя.

А ведь такое поведение характерно в первую очередь для распространения вредоносного программного обеспечения. Множество пользователей получают ссылку на вредоносный файл и, увы, пытаются его запустить. А при посещении зараженной страницы вполне возможна попытка запуска вредоносного кода (в этом случае используются лазейки браузера и другого программного обеспечения).

Как же пользователю понять, стартует легитимный процесс обновления или это вредоносный код? В данном случае может помочь информация о запуске,

получаемая из «облачной» сети. Ведь поведение программы анализируется как обычными методами проактивной защиты, так и с помощью серверов «Лаборатории Касперского».
Информация о запуске новых версий легитимного файла или же вредоносного кода накапливается в «облачной сети», и одновременно с этим поведение программы анализируется стандартными методами защиты. Если программа ведет себя подозрительно, например пытается изменить системные файлы или получить несанкционированный доступ к пользовательской информации, сообщение об этом также поступает в «облако». В результате выносится вердикт — является программа опасной или нет.
Что произойдет, если программа все же оказалась вредоносной? Пользователи, попытавшиеся запустить ее, в первые минуты атаки будут защищены с помощью проактивных методов. Все остальные участники Kaspersky Security Network оперативно получат информацию о новой угрозе и будут предупреждены при попытке запуска соответствующего файла. Кроме того, данные поступят в распоряжение экспертов «Лаборатории Касперского» для последующего анализа.

«Облако» в ручном режиме

«Облачная» система безопасности работает в полностью автоматическом режиме. В 2012-х версиях программ Kaspersky Internet Security и Kaspersky Anti-Virus процесс работы с «облаком» стал более информативным. В специальном окне программы теперь доступны актуальные сведения о работе Kaspersky Security Network.
Пользователю доступна статистика работы «облака» за последние 24 часа. В приведенном примере за этот отрезок времени KSN защищала более полутора миллионов пользователей, благодаря чему было нейтрализовано свыше 11 млн случаев вредоносных атак.
Кроме того, появилась возможность использовать функции «облачной» системы в ручном режиме. С помощью специального пункта в контекстном меню вы можете оценить репутацию любого исполняемого файла на своем компьютере. Для этого достаточно щелкнуть правой кнопкой мыши по интересующей вас программе и выбрать пункт Check Reputation in KSN.
Можно ли использовать только «облачное» решение?
Возможно ли оставить на своем компьютере только «облачное» решение? Будет ли этого достаточно? Некоторые производители антивирусного программного обеспечения считают, что да (решение Panda Cloud Antivirus). На мой взгляд, это не совсем верно. Почему?
С одной стороны, это решение слишком «идеально». Практически мгновенная реакция на новые угрозы, отсутствие нагрузки на локальные компьютеры. В реальности это не так, и на то есть несколько причин.
Во-первых, чем быстрее пополняется «облачная» коллекция, тем более эффективную защиту «облако» может представить. Естественно, для того чтобы ее обработать, нам нужен клиент на пользовательской стороне. Источники в данном случае такие:

- специальные вирусные ловушки, организованные антивирусными лабораториями;

- обмен экземплярами вредоносного кода между различными антивирусными компаниями;
- информация, поступающая с компьютеров пользователей KSN.

Во-вторых, если ваш компьютер не подключен к Интернету, «облачная» защита просто не работает. Но ведь источники заражения (локальная сеть, USB-носители и т. п.), увы, никуда не исчезают. Сегодня, по данным «Лаборатории Касперского», при наличии интернет-соединения с помощью «облачных» технологий отсекается 30% вирусных заражений. А остальные можно предотвратить только с помощью локального продукта.

Вывод отсюда прост. Продукт, обеспечивающий антивирусную защиту на компьютере пользователя, просто необходим, поскольку:

- он обеспечивает защиту при отсутствии подключения к Интернету;
- если заражение все же произошло, вылечить компьютер через Сеть зачастую невозможно, так как вредоносное программное обеспечение может просто блокировать соединение с Интернетом.

Итак, средства защиты, не использующие «облачные» технологии, сегодня уже не актуальны. Однако следует понимать, что сегодня производители антивирусного программного обеспечения не в состоянии перенести всю защиту в «облако», так как существует огромное количество угроз не только из Интернета. Реально работающим может быть лишь решение, сочетающее в себе мощную клиентскую составляющую с устойчивой «облачной» службой.

Фактически «облако», получая всю актуальную информацию об угрозах и безопасных объектах, передает ее на централизованные серверы в реальном времени. Выработанные на основе этой информации средства защиты или данные о безопасных объектах поступают в KSN на миллионы пользовательских компьютеров. Таким образом, на них не нужно проводить ресурсоемкий анализ, что позволяет минимизировать ложные срабатывания и защищать компьютеры от новейших угроз еще до выпуска соответствующих сигнатур.

В то же время при отсутствии подключения к Интернету компьютер по-прежнему защищен, ведь на нем остается полнофункциональный антивирус.

Владимир Безмалый (vladb@windowslive.com) — специалист по обеспечению безопасности, MVP Consumer Security, Microsoft Security Trusted Advisor