Прогноз? Облачно!

Безмалый В.Ф.

MVP Consumer Security

Microsoft Security Trusted Advisor

Введение

В последнее время все чаще и чаще мы читаем и слышим о таком понятии как «облачные» технологии. Но почему-то большинство не только пользователей, но и ИТ считают что это нечто весьма далекое и применять эти технологии мы будем еще очень и очень не скоро. Это не так. Более того, многие из нас уже успешно применяют данные технологии, абсолютно не задумываясь при этом о том, что они используют.

В данной статье речь пойдет об «облачных» технологиях безопасности, применяемых сегодня пользователями на своих домашних и не только домашних ПК:

- Антивирусное «облако»
- Сервис репутации

Антивирусное «облако»

Для упрощения инфраструктуру антивирусной компании, которая используется для обработки информации, полученной с компьютеров пользователей персонального продукта, и выявляет новые недетектируемые угрозы, мы назовем антивирусным «облаком». Я понимаю желание читателей мне возразить, однако такая практика применения термина уже сложилась.

Предпосылки создания

Изначально для антивирусной защиты пользователей использовался сигнатурный и эвристический анализ объектов, потому что:

- Вирусы появлялись относительно редко;
- Скорость реакции, обеспечиваемая обычными обновлениями, устанавливаемыми на компьютеры пользователей, удовлетворяла требованиям безопасности.

Однако с ростом числа подключений и скорости подключения к сети интернет возникла возможность завладеть деньгами пользователей, создавать различный ботнет сети и т.д. Появился веский аргумент для активного развития написания вредоносного кода. По данным специалистов Лаборатории Касперского, в 2007 году количество вредоносного ПО составляло менее 5 млн экземпляров, а в 2009 уже почти 20 млн. Естественно, это привело к существенному увеличению объема антивирусных обновлений, что вызывает заметные неудобства для пользователей. Так, по данным специалистов Лаборатории Касперского, в 2007 году объем обновлений составлял порядка 15 мегабайт за год, в 2010 году этот показатель увеличился до 130 Mb.

По данным исследования, проведенного во втором квартале 2010 года компанией NSS Labs, время, необходимое антивирусным компаниям для блокирования web-угроз, составляет от 4,62

до 92,48 часа (http://nsslabs.com/host-malware-protection/q2-2010-endpoint-protection-product-group-test-report.html). Дальнейшее принципиальное увеличение максимальной скорости реакции на угрозы с помощью обычных антивирусных обновлений невозможно, так как затраты времени на обнаружение зловредов, их последующий анализ и тестирование формируемых антивирусных обновлений уже сведены к минимуму.

Если же говорить об эвристическом анализе, то не стоит забывать, что уровень обнаружени при этом составляет максимум 50-70%.

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?

Одним из методов решения возникших вопросов стало появление антивирусного «облака».

Как это работает?

Рассмотрим, как это работает на примере Kaspersky Security Network.

В отличие от стандартного процесса обновления баз антивирусных сигнатур, когда общение с пользователями проходит в одном направлении (от сервера к пользователю), в случае использования «облачных» технологий мы имеем двунаправленное общение. Как от сервера к пользователю, так и от пользователя к серверу.

В случае системы обновлений антивирусных баз обратной связи от пользователя к серверу нет, поэтому антивирусная лаборатория не может получать оперативную информацию о заражении, его источниках и распространении вредоносного ПО. До недавнего времени подобная информация попадала в антивирусные лаборатории с задержкой, что приводило к распространению вредоносного ПО и эпидемиям.

При использовании «облачных» технологий связь двусторонняя. Множество пользовательских ПК сообщают в «облако» о подозрительной активности. В случае обнаружения подозрительной активности, информация об этом сразу же становится известной антивирусной лаборатории. После обработки данная информация становитс яизвестна пользовательским ПК, подключенным к «облаку». Фактически пользователи оперативно делятся последством «антивирусного облака» информацией о проводимых против них атаках вредоносного ПО и источниках таких атак, что позволяет гораздо быстрее блокировать их. Таким образом мы имеем единую интеллектуальную антивирусную сеть.

Ключевым отличием «облачных» технологий является то, что в данном случае пересылается не сам файл, а его метаданные: хеш-функция, информация о поведении, источник появления и т.д., при этом сами файлы в «облако» не передаются.

В частности, при согласии пользователя участвоватьв Kaspersky Security Network (KSN) на серверы «Лаборатории Касперского» отправляются следующие металанные:

- информация о заражениях, либо атаках на пользователя;
- информация о подозрительной активности исполняемых файлов на компьютере пользователя.

Указанная информация передается только с согласия пользователя. После этого экспертная система выявляет угрозы, проверяет качество принятых решений, после чего осуществляется

поиск источников угроз. Найденные источники также проходят проверку, а после этого информация, полученная экспертной системой, становится доступной всем пользователям KSN.

Несомненным преимуществом использования «облачных» технологий является скорость реакции. Если обновление сигнатур требует нескольких часов, то на выявление и детектирование новых угроз с помощью «облачных» технологий нужны минуты.

Использование фильра SmartScreen

Второй технологией безопасности, которую использует огромное количество пользователей, является фильтр SmartScreen, встроенный в Internet Explorer, начиная с версии 8.

Как показывает анализ SmartScreen Filter, каждая четырнадцатая программа, загружаемая пользователями Windows, является вредоносной, однако около 5% пользователей игнорируют предупреждения и скачивают опасные приложения.

Ежечасно SmartScreen блокирует более 125 тыс. потенциально небезопасных сайтов и программ.

Каждую минуту выполняется почти 2 тыс. потенциально опасных загрузок.

Фильтр SmartScreen в Internet Explorer предупреждает пользователя о подозрительных или уже известных мошеннических веб-узлах. При этом фильтр проводит анализ содержимого соответствующего сайта, а также использует сеть источников данных для определения степени надежности сайта. Фильтр SmartScreen сочетает анализ веб-страниц на стороне клиента на предмет обнаружения подозрительного поведения с онлайн-службой, доступ к которой пользователь разрешает или запрещает. При этом реализуется три способа защиты от мошеннических и вредоносных узлов.

1. Сравнение адреса посещаемого сайта со списком известных сайтов. Если сайт найден в этом списке, больше проверок не производится.
2. Анализ сайта на предмет наличия признаков, характерных для мошеннических сайтов.
3. Отправка адреса сайта, на который пользователь собирается зайти, онлайн-службе Microsoft, которая ищет сайт в списке фишинговых и вредоносных сайтов. При этом доступ к онлайн-службе производится асинхронно по SSL-соединению, так что это не сказывается на скорости загрузки страниц.

С помощью Internet Explorer вы можете узнать, является ли узел мошенническим. Для этого выберите из меню «Безопасность» пункт Фильтра SmartScreen, а затем «Проверить веб-узел».

Работа фильтра SmartScreen основывается на службе Microsoft URL Reputation Service (URS), осуществляющей круглосуточную поддержку. Если фильтр SmartScreen включен, то он просматривает локальный список известных разрешенных узлов и отправляет адрес URL узла службе URS для проверки.

Во избежание задержек обращения к URS производятся асинхронно, так что на работе пользователя это не отражается. Чтобы уменьшить сетевой трафик, на клиентском компьютере хранится зашифрованный DAT-файл со списком тысяч наиболее посещаемых узлов; все включенные в этот список узлы не подвергаются проверке фильтром SmartScreen. В фильтре SmartScreen также применяется механизм локального кэширования адресов URL, позволяющий сохранять ранее полученные рейтинги узлов и избежать лишних обращений по сети. Один из способов выявления потенциально подставных узлов, применяемый службой URS, — сбор отзывов пользователей о ранее неизвестных узлах. Пользователь может решить, следует ли отправлять информацию об узле, который вызывает у него подозрения.

Для защиты от фишинга и эксплойтов фильтр SmartScreen исследует строку URL целиком, а не подмножество адресов URL, на которые заходил пользователь. Учтите, что службе URS могут быть переданы личные сведения, поскольку иногда они находятся в самой строке URL.

Фильтр SmartScreen можно включать или отключать избирательно для каждой зоны безопасности, но только в том случае, когда эта функция включена глобально. По умолчанию фильтр SmartScreen включен для всех зон, кроме местной интрасети. Если вы захотите исключить некоторые узлы из списка проверяемых фильтром SmartScreen, но не отключать при этом фильтр полностью, то необходимо включить фильтр глобально, а затем отключить фильтрацию только для зоны «Надежные узлы», после чего конкретные узлы добавить в эту зону.

Вывод

Является ли использование «облачных» технологий безопасности универсальным способом защиты? Безусловно нет! Большая работа по обеспечению безопасности по прежнему проводится на ПК пользователя, однако использование «облачных» технологий позволяет существенно ускорить процесс. Ну и не стоит забывать о скорости и качестве интернет-соединения. Ведь самая хорошая «облачная» структура практически бесполезна, если у вас нет связи.