«Облачные» технологии в антивирусной защите

Владимир Безмалый

Сегодня рост вредоносного программного обеспечения становится лавинообразным. 70 тыс. экземпляров в день — и это не предел! Появление вредоносного программного обеспечения на планшетах и смартфонах уже никого не удивляет. Все это способствует тому, что традиционных средств антивирусной защиты, таких как проактивная защита и сигнатурный анализ, становится недостаточно для обеспечения безопасности.

В индустрии долгое время формировался более-менее понятный механизм обеспечения защиты, при котором от пострадавшего пользователя или из другого источника в лабораторию присылался образец вредоносного кода, и после проведения всестороннего анализа антивирусная лаборатория выпускала обновление баз сигнатур вместе с рецептом удаления «заразы». Все клиенты загружали это обновление и получали соответствующую защиту. Естественно, кто-то заражался раньше, чем получал «лекарство». Но таких было не так уж много. Однако шло время, количество угроз росло. Производителям антивирусного программного обеспечения пришлось максимально автоматизировать процесс анализа новых угроз, используя эвристические механизмы, и даже встроить подобные механизмы в сами клиентские антивирусы. При этом частота выпуска обновлений непрерывно росла. Выпуски стали вначале ежедневными, а потом даже ежечасными.

Однако, несмотря на успехи производителей антивирусов, стало понятно, что экспоненциальный рост числа новых угроз не оставляет подобному подходу ни одного шанса. С одной стороны, антивирусные компании не могут наращивать ресурсы такими же темпами, с другой — объем выпускаемых обновлений выходит за пределы разумного.

В свое время в антивирусной индустрии бытовало мнение, что описанную проблему раз и навсегда решат эвристические технологии, то есть методики детектирования не на основе сигнатуры, а с использованием методов искусственного интеллекта, встраиваемого в антивирус. Эти технологии получили широкое распространение, но проблемы решить не смогли. Лучшие примеры реализации эвристического анализа обеспечивают уровень обнаружения в пределах 50–70% для знакомых семейств вирусов и совершенно бессильны перед новыми видами атак.

На сегодня сформировалось мнение, что распознавать угрозы необходимо непосредственно в распределенных центрах обработки данных антивирусной компании, а не только на компьютере конечного пользователя. Такой перенос «центра тяжести» технологии в Интернет и называется «облачным».

Переход к «облачным» технологиям позволяет упростить архитектуру продукта, который пользователь ставит на свой компьютер, ведь теперь для каждого подозрительного ресурса предоставляется небольшое по объему обновление, индивидуально загружаемое из «облака» практически

ИЛЛЮСТРАЦИЯ MAXIM_KAZMIN© - FOTOLIA.COM

в реальном времени. Разумеется, разработанные технологии существенно сложнее, ведь многие процессы в компьютере требуют реакции более быстрой, чем скорость получения подобных обновлений. Кроме того, необходимо обеспечить защиту в тот момент, когда компьютер вообще не подключен к Интернету. Тем не менее «облачные» технологии являются ключом к обеспечению безопасности не самых мощных компьютеров, таких как нетбуки, планшеты и смартфоны.

По данным исследования, проведенного во втором квартале 2010 года компанией NSS Labs, время, необходимое антивирусным компаниям для блокирования веб-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 вирусов, их последующий анализ и тестирование формируемых антивирусных обновлений уже сведены к минимуму.

Как быть?

В таких условиях необходим качественный скачок в индустрии безопасности. Его и обеспечили «облачные» технологии защиты. Сегодня в состав многих антивирусов входит «облачная» составляющая. В частности, свои «облака» имеют компании Trend Micro, Kaspersky Lab, Symantec, McAfee, Avast! и другие. Более того, как мне кажется, в скором времени либо все существующие лаборатории перейдут к использованию подобных технологий, либо кто-то из них будет вынужден просто покинуть рынок. В данной статье мы рассмотрим антивирусные «облака» двух компаний: Trend Micro и «Лаборатории Касперского».

Trend Micro SPN

Первым масштабным проектом по переносу антивирусной защиты в «облако» было построение компанией Trend Micro системы Smart Protection Network. Ключевой идеей этой системы была концепция «репутации» — вынесения вердикта для ресурса (файла, сайта, сообщения электронной почты) только на основе накопленных ранее данных, то есть без необходимости анализировать сам ресурс непосредственно в момент обращения к нему пользователя. На первый взгляд такая идея кажется странной, но на самом деле это единственный подход, который позволяет автоматически отражать неизвестные угрозы в автоматическом режиме. Другие подходы, которые анализируют сам ресурс, могут основываться только на исследовании эксперта либо на эвристических алгоритмах. В современных условиях оба традиционных подхода становятся все менее эффективными. Ручной анализ за последние несколько лет потерял актуальность с ростом числа угроз, а эвристика не успевает за увеличением числа вариаций вредоносных кодов и других приемов злоумышленников.

Рисунок 1 Trend Micro Smart Protection Network

В SPN используется несколько методов отслеживания репутации. Первый и самый очевидный — это формирование базы ресурсов, например сайтов, и отслеживание происходящих изменений. Чем-то этот подход похож на методику поисковых систем, но цели преследуются совсем иные, соответственно и данные собираются другие. Если, например, сайт слишком часто меняет IP-адрес, то это типичный признак вредоносного сайта. При этом в чем, собственно, заключается его вредоносность — неизвестно. Сайт может распространять вредоносный код или представлять собой ложный сайт какого-нибудь банка. В общем, пользователю это не важно. Главное, что при попытке посетить данный сайт антивирус Trend Micro в реальном времени сверяется с SPN, и доступ блокируется.

Кроме базы репутации сайтов, SPN хранит базу репутации источников сообщений электронной почты, а также базу репутации отдельных файлов. Использование последней чаще всего называют «облачным» антивирусом. Но именно наличие всех трех баз обеспечивает второй и самый хитрый способ выявления угроз. Разработчики Trend Micro называют этот метод корреляцией. Суть его в том, что с помощью взаимосвязи данных во всех трех базах формируется профиль защиты (см. рисунок 1).

Trend Micro Smart Protection Network состоит из нескольких ключевых компонентов, которые позволяют защитить пользователей от вредоносного контента в реальном времени.

- Web Reputation — «облачная» служба, которая использует базы данных репутации доменов для

Рисунок 2 Архитектура Web Reputation

отслеживания надежности URL, страниц и объектов путем присвоения рейтинга репутации на основе таких факторов, как возраст веб-сайта, изменение расположения и сведения о подозрительных действиях, обнаруженные в ходе анализа вредоносного поведения. Репутации определяются и обновляются на основе постоянного анализа. При этом вредоносное содержимое будет заблокировано после анализа в «облаке», до того, как вредоносный код достигнет устройства пользователя.

- Email Reputation — «облачная» служба, применяющая технологию репутации для проверки IP-адреса, используя репутацию известных спам-адресов. Репутация определяется путем последовательного анализа поведения IP-адреса, сферы деятельности и предыдущей истории. Email Reputation блокирует вредоносные письма в «облаке» на основе IP-адреса отправителя и предотвращает их попадание на компьютер пользователя.
- File Reputation — технология File Reputation обеспечивает масштабируемый и эффективный способ быстрого блокирования вредоносного программного обеспечения в «облаке», прежде чем оно достигнет устройства конечного пользователя.
- Корреляция анализа поведения — корреляция по обратной связи. При этом коррелируются данные о деятельности из нескольких источников Trend Micro Smart Protection Network для выявления вредоносного контента, который не может быть обнаружен с помощью одного источника. Запатентованный двигатель корреляции использует анализ Web, электронной почты, файлов, вирусов, программ-шпионов, фарминг, фишинг и другие механизмы анализа, позволяя выявить активность от сложных и скрытых атак, чтобы дать клиентам Trend Micro явное преимущество в степени защищенности.
- Smart Feedback — каналы обратной связи, которые обеспечивают непрерывное взаимодействие между продуктами Trend Micro и самой антивирусной компанией. «Облако» обновляется в режиме 24/7. Таким образом, угроза, найденная на компьютере одного из пользователей, автоматически будет добавлена в «облако», и о ней станет известно другим пользователям практически в реальном времени.

На сегодня Trend Micro поддерживает работу пяти центров обработки данных в разных регионах по всему земного шару, обрабатывая при этом более 7,2 Тбайт данных ежедневно. Деятельность Trend Micro обеспечивают более 2000 экспертов в области безопасности, работающих по всему миру в режиме 24/7.

Как работает Web Reputation

Служба Web Reputation использует одну из крупнейших в мире баз репутаций доменов для отслеживания надежности веб-сайтов, страниц и страничных объектов (например, ссылок). Репутация каждого элемента позволяет сделать вывод, чтобы создать политику, на основе которой будет разрешен или запрещен соответствующий контент на основе рейтинга репутации.

При этом применяется гибридный подход к обеспечению сканирования интернет-контента, то есть используются в качестве «облачных» такие службы, как инфраструктура Smart Protection Network, служба Web Reputation и фильтрации URL-адресов и сканирования на локальном компьютере, чтобы обеспечить максимально высокий уровень обнаружения вредоносных программ (см. рисунок 2).

Ключевые компоненты и функции Web Reputation

- Dual Band Service — поддерживаются как возможности поиска в DNS и HTTP. По умолчанию поиск HTTP обращается к «облачной» службе Web Reputation для запроса репутации из базы. Исходя из запроса, база данных Web Reputation Service (WRS) возвращает очки репутации. DNS-запросы используются для запроса репутации домена.
- Rating Parameters — каждая служба Web Reputation использует широкий ряд номинальных параметров, чтобы определить, является ли объект, расположенный на веб-сайте, вредоносным. Инфраструктура Smart Protection Network использует несколько сотен параметров рейтинга между ее ключевыми компонентами для точного определения контента веб-сайтов. Оценка параметров для веб-службы репутации может включать проверку следующих параметров:
  - Что такое возраст домена?
  - Что такое стабильность истории IP-адреса?
  - Связан ли данный сайт с любым другим известным вредоносным сайтом?
  - Является ли содержание частью фишинговой или фарминг-сущности?
  - Не содержит ли URL-ссылку, связанную с известным ботнетом?
- URL Filtering Categorization — служба фильтрации соотносит свои рейтинги безопасности категории с базой данных WRS, чтобы обеспечить широкий спектр защиты.
- Smart Feedback — Web Reputation широко использует обратную связь от всех продуктов Trend Micro. Это обеспечивает обнов-

ление оценки репутации в реальном времени.

- Page Analysis — используется проверка на клиентском компьютере, чтобы убедиться, что с момента последней проверки страницы она не была изменена и контент не был подменен. Анализ страницы обеспечивает обнаружение быстро меняющихся и скрытых угроз и защищает от «угроз нулевого дня». О любом найденном вредоносном содержимом будет немедленно уведомлена служба Web Reputation для повторного анализа и пересчета репутации.

Вредоносное содержимое может быть блокировано на основе оценки содержимого службы Web Reputation. При этом могут быть использованы следующие балльные пороги (см. таблицу).

Таблица. Система баллов службы Web Reputation

Уровень репутации	Баллы	Описание
High	>80	Известный хороший сайт
Medium	>65	Сайт замечен в спаме, имеет низкую стабильность, отмечались нарушения
Low	>50	На сайте обнаружена вредоносная программа, фишинговые страницы

Антивирусное «облако» Kaspersky Security Network

Эта «облачная» система безопасности была создана для максимально оперативного реагирования на новые угрозы в 2008 году и с тех пор является одной из ключевых технологий защиты компьютерных устройств в продуктах «Лаборатории Касперского». Главная особенность этого подхода заключается в том, что ключевой вклад в борьбу с новыми угрозами вносят сами пользователи. При установке продукта «Лаборатории Касперского» пользователю явно предлагают согласиться на передачу данных о запускаемых программах в «облако». Эти данные полностью анонимны, но они позволяют определить новое вредоносное программное обеспечение и оповестить остальных пользователей программ «Лаборатории Касперского» буквально в течение нескольких минут.

Как это работает?

Начнем с того, что основная задача антивируса — предотвратить появление на компьютере вредоносных программ. К сожалению, на современном компьютере новые программы появляются регулярно. Даже если сам пользователь ничего не устанавливает, многие уже установленные программы (продукты компании Adobe, Apple, Google и т. д.) автоматически обновляются, загружая из Интернета свои новые версии. Это очень удобно для пользователя, но осложняет задачу антивирусу. Ведь распространение нового вируса или троянской программы происходит сходно: в системе «вдруг» появляется новая программа. В случае с вредоносным кодом чаще всего сценарий следующий: множество пользователей получают ссылку на вредоносный файл в социальных сетях, по электронной почте или через систему мгновенного обмена сообщениями и, увы, пытаются его загрузить и запустить. Более того, часто при посещении специальной страницы запуск вредоносного кода происходит автоматически. В таких случаях используются уязвимые места в браузере и других программах. 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 только с помощью поведенческого анализа, который способен выявить «подозрительную» активность. Все остальные участники KSN оперативно получат информацию о новой угрозе и будут предупреждены при попытке запуска соответствующего файла. Данные также поступят в распоряжение экспертов «Лаборатории Касперского» для последующего анализа.

Такой подход принципиально отличается от традиционного. При традиционном обновлении антивирусных баз обратной связи от пользователя к серверу нет, поэтому антивирусная лаборатория не получает информацию о факте заражения, его источниках и распространении вредоносного программного обеспечения.

Отметим, что использование KSN обладает и другими преимуществами, кроме оперативной реакции на новые угрозы: в лабораторию никогда не пересылается сам подозрительный файл, а только его свойства: хэш-функция, информация о поведении, источник и т. д. Таким образом, у пользователя не должно возникать беспокойства по поводу утечки данных. Так что, если вы используете продукт «Лаборатории Касперского», настоятельно рекомендуется не отключать функции KSN. В случае если подозрительный файл все же признается вредоносным, он может быть передан в «Лабораторию Касперского» для дополнительного обследования и принятия окончательного решения.

Использование «облачных» технологий позволило реализовать с помощью Kaspersky Security Network следующие функции.

Веб-фильтр. Веб-фильтр предназначен для ограничения доступа к вредоносным и мошенническим интернет-ресурсам. Веб-фильтр проверяет ссылки на веб-страницах. Рядом с ними выставляются значки разного цвета в соответствии с категорией опасности. Сайты делятся на опасные, безопасные и недостаточно известные. В первую очередь ссылки проверяются в локальной

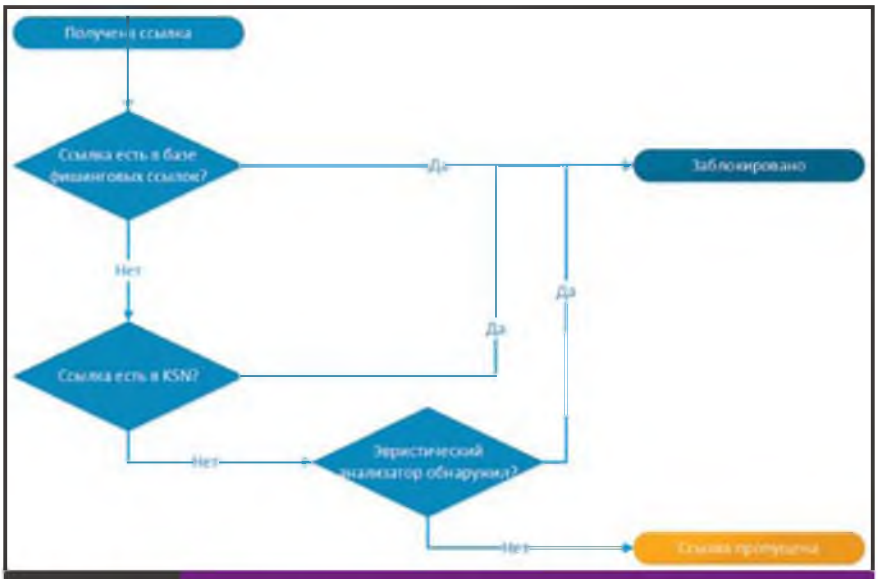

Рисунок 3 Блок-схема поиска фишинговой ссылки

базе фишинговых и вредоносных сайтов. После этого поиск ведется в черных списках системы KSN. Если ресурс неизвестен и там, применяется эвристический анализ на наличие фишинговых ссылок.

Анти-фишинг. В ходе анализа производится проверка по базе фишинговых ссылок, Kaspersky Security Netwok (KSN) и эвристическим модулем. Если в ходе анализа хотя бы одним из модулей ссылка признается фишинговой — она блокируется (см. рисунок 3).

Отмечено, что применение KSN обеспечивает высокую скорость оповещения пользователей о фишинговой угрозе. При обнаружении нового вредоносного объекта на компьютере любого из пользователей KSN информация о данном вредоносном объекте становится доступной для всех остальных пользователей KSN через 40 секунд после его обнаружения, а уже через час на компьютере пользователя обновляются антифишинговые базы.

Эвристический модуль осуществляет классификацию в соответствии с набором признаков. Всего на сегодня количество признаков для анализа уже превышает сто. В ходе анализа выделяются признаки из HTML и URL, затем они отправляются в специальный модуль, который выдает вердикт на основании существующих обучающих наборов. Например, к анализируемым признакам страницы можно отнести наличие на странице подозрительной лексики, наличие форм ввода, URL содержит нечитаемые последовательности символов.

Kaspersky Security Network (KSN) — это служба, предоставляющая доступ к базе знаний «Лаборатории Касперского» о репутации файлов, интернет-ресурсов и программного обеспечения. Для вычисления репутации того или иного URL используется несколько источников.

1. Непосредственно пользователи продукта, которые обращаются с просьбами о категорировании того или иного нового веб-ресурса (URL).
2. Файлы зон — списки всех доменов, высокоуровневых доменов таких как com, net, info. Информация предоставляется по договору с регистратором.
3. Поисковые выдачи. Роботы запрашивают у различных поисковых машин наборы ключевых фраз. На выходе имеем наборы сайтов, которые ставятся в очередь на проверку.

Обработка фишингового запроса в сети KSN показана на рисунке 4.

Обработка фишингового запроса производится следующим образом:

1. По запросу в KSN проводится обнаружение ссылки в URL Reputation Service.
2. Если ссылка обнаружена, то атака не удалась, ссылка блокирована.
3. Если ссылка не обнаружена в KSN, производится эвристический анализ соответствующей страницы.
4. Если ссылка признана вредоносной, то производится ее публикация в KSN.
5. Кроме того, обновление базы вредоносных ссылок в KSN производится по результатам работы групп аналитиков вредоносного программного обеспечения, а также аналитиков контентной фильтрации.

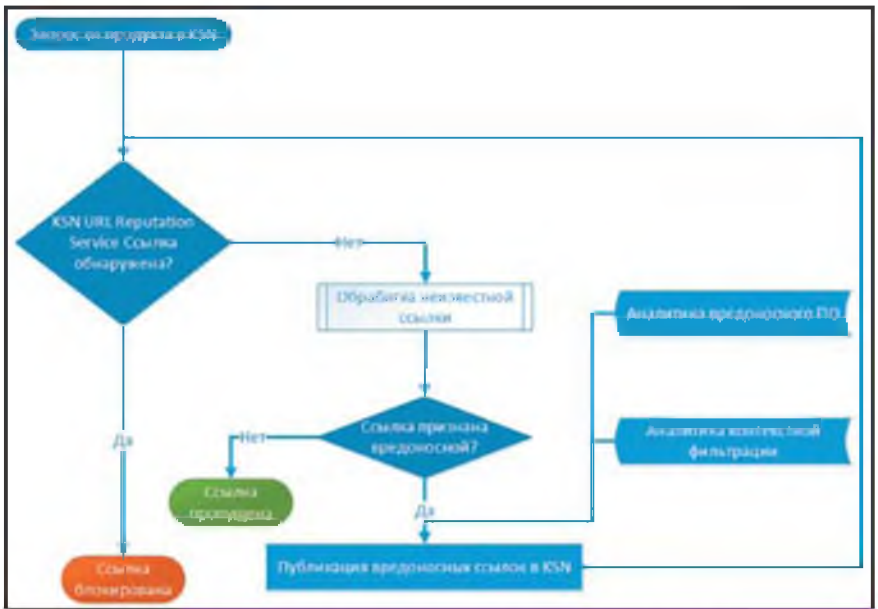

Рисунок 4 Обработка фишингового запроса в KSN

6. При этом выполняется тщательный анализ и проверка полученных результатов.
7. После этого происходит публикация вредоносных ссылок в KSN и обновление базы вредоносных ссылок на компьютерах пользователей.

Анти-Спам. Если ранее требовалось обучить антиспамовый модуль на некотором количестве писем перед началом работы, то сейчас такое обучение не требуется, поскольку информация для работы модуля берется из «облака», где уже имеется актуальная база образцов спам-сообщений. Из баз Kaspersky Security Network на пользовательские компьютеры поступают шаблоны новых рассылок спама и новые адреса вредоносных, спамерских и фишинговых ресурсов. Это позволяет быстро приспосабливаться к изменениям тактики спамеров и налаживать адекватную защиту.

Контроль программ. Система Kaspersky Security Network участвует в определении рейтингов опасности программ. Такие рейтинги используются при назначении прав доступа различного программного обеспечения к ресурсам компьютера и персональным данным пользователя. В Kaspersky Internet Security 2012 информация о новом программном обеспечении поступает сразу из нескольких источников: системы KSN и различных компонентов обновленных продуктов, таких как «Контроль программ», «Мониторинг активности программ» и «Эвристический анализатор». Активный обмен данными обеспечивает максимальную полноту и актуальность анализируемой информации.

Проверка репутации программ. Всего один раз нажав клавишу мыши, пользователь Kaspersky Internet Security 2013 может узнать репутацию любого исполняемого файла на локальном компьютере и решить, стоит ли его использовать. Для этого нужно лишь кликнуть правой кнопкой мыши по иконке файла и выбрать в контекстном меню опцию «Посмотреть репутацию в KSN». Но даже если этого не сделать, все необходимые проверки будут проведены автоматически. Информация о каждой программе мгновенно попадает в «облачную» сеть, даже если эта программа только что появилась в Интернете.

«Облачный» вариант

Итак, преимущества использования «облачных» технологий для защиты пользователя очевидны:

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

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