Прогноз? Облачно!

Безмалый В.Ф.

MVP Consumer Security

Microsoft Security Trusted Advisor

Кондрашин М.П.

Trend Micro Certified Security Master

Введение

В последнее время все чаще и чаще мы читаем и слышим о таком понятии как «облачные» технологии. При этом большинство пользователей считают что это нечто весьма далекое и практическое применение этих технологии, вопрос завтрашнего дня. На самом деле, это не так. Облачные технологии уже широко применяются. Более того, многие из нас уже успешно используют данные технологии, не зная об этом.

В данной статье рассмотрим, облачные технологии, которые используются в продуктах для защиты домашних и не только домашних ПК.

Предпосылки переноса безопасности в облака

Ключевым фактором, который привел к необходимости пересмотреть подходы к обеспечению безопасности пользователей, является значительный рост числа уникальных образцов вредоносного кода. Тенденция последние несколько лет была неутешительна – темпы роста носили экспоненциальный характер. Например, по данным независимой тестовой лаборатории AV-test, количество собранных ими образцов увеличилось в прошлом году почти вдвое — 20 миллионов, против 12 миллионов в 2009. Такая динамика дает предсказания, которые рушат все традиционные представления о том, как действует средство защиты.

С начала антивирусной индустрии сложился понятный механизм обеспечения защиты, когда от пострадавшего пользователя или из другого источника лаборатория получала образец вредоносного файла и после всестороннего анализа выпускала обновления к базе сигнатур вирусов вместе с рецептом по удалению заразы. Все клиенты загружали это обновление и получали актуальную защиту. Разумеется, что была доля тех, кто заражался раньше, чем получал обновление, но таких было относительно мало. По мере роста числа угроз, производителям антивирусов пришлось максимально автоматизировать процесс анализа новых видов угроз, используя эвристические механизмы и даже встроить подобные механизмы в сами антивирусы. При этом частота обновлений увеличилась и выпуски стали ежедневными и даже ежечасными.

Несмотря на успехи антивирусных компаний в описанных способах ускорения выпуска обновлений, очевидно, что экспоненциальный рост числа новых угроз не оставляет этому подходу шанса. С одной стороны, антивирусные компании не в силах наращивать человеческие ресурсы такими же экспоненциальными темпами. С другой стороны, объем выпускаемых обновлений выходит за все разумные пределы.

Одно время в индустрии безопасности бытовало мнение, что описанную проблему раз и навсегда решат, так называемые, 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 совершенно новыми видами атак.

В настоящий момент сформировалось общее видение, что поле борьбы с угрозами, которое сводится к тому, 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 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 в реальном времени. Разумеется, что разработанные технологии существенно сложнее, ведь многие процессы в компьютере требуют времени реакции выше, чем скорость получения подобных обновлений. Кроме этого, необходимо обеспечить защиту в тот момент, когда компьютер вообще не подключен к Сети. 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 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.

Антивирусное «облако» Kaspersky Security Network

Одной из реализаций облачного подхода стала Kaspersky Security Network (KSN). 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 ПК в продуктах «Лаборатории Касперского». Главное отличие этого подхода от других используемых средств защиты заключается в том, что ключевой вклад в борьбу с новыми угрозами дают сами пользователи. Разумеется, что такую помощь от пользователя продукт получает не без спроса. 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 ПО и оповестить всех других пользователей программ «Лаборатории Касперского» буквально в течение нескольких минут.

Как это работает?

Начнем с того, что основная задача антивируса заблокировать появление на компьютере вредоносных программ. К сожалению, на современном компьютере регулярно появляются новые программы. Даже если сам пользователь ничего не устанавливает, многие уже установленные программы (продукты компании Adobe, Apple, Google и т.д.) автоматически обновляют себя, загружая из Интернета свои новые версии. Это очень удобно для пользователя, но осложняет работу 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 обмена мгновенными сообщениями, и, увы, пытаются его загрузить и запустить. Более того, часто при посещении специальной вредоносной страницы запуск вредоносного кода происходит автоматически — без ведома пользователя. В таких случаях задействуются уязвимости 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 ли 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 ПО.

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: хеш-функция, информация о поведении, источник появления и т.д. Таким образом, у пользователя не должно возникать никаких беспокойств по поводу утечки приватных данных. Так что если вы использует продукт Лаборатории Касперского, то мы настоятельно рекомендуем не отключать функции KSN.

Trend Micro SPN

Первым масштабным проектом по переносу антивирусной защиты в облако, было построение Smart Protection Network компанией Trend Micro. Ключевой идеей этой системы была концепция “репутации”, то есть 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 эта 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 ручном исследовании эксперта, либо на эвристических алгоритмах. В современных условиях, оба этих традиционных подхода становятся все менее и менее эффективными. Ручной анализ потерял актуальность за последние несколько лет с ростом числа угроз, а эвристика не успевает за ростом вариаций вредоносных кодов и других изощренных приемов злоумышленников.

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 тут преследуются совсем иные,

соответственно и данные собираются другие. Если, например, сайт слишком часто меняет свой IP-адрес, то это типичный признак вредоносного сайта. При этом в чем собственно заключается его вредоносность не известно. Сайт может распространять вредоносный код или представлять собой подложный сайт какого-нибудь банка. В общем-то, пользователю это не важно. Главное, что при попытке посетить этот сайт, антивирус Trend Micro в реальном времени сверяется с SPN и блокируется доступ.

Кроме базы репутации сайтов, SPN хранит базу репутации источников сообщений электронной почты, а также базу репутации отдельных файлов. Именно использование последней чаще всего называют облачным антивирусом. Но именно наличие всех трех баз, дает второй и самый изощренный способ выявления угроз. Разработчики Trend Micro называют этот метод корреляцией. Суть метода в том, что используя по информацию в одних базах наполняются другие. Опять же воспользуемся примером, с тем, чтобы пояснить данную методику.

Рассмотрим сообщение электронной почты, которое приходит в ловушку для спама в TrendLabs с известного источника спама. Если к сообщению прикреплен исполняемый, то с него снимается контрольная сумма и она пополняет базу репутации файлов. Одновременно этот файл автоматически запускается в контролируемом окружении и выявляется, например, что он загружает из Интернета еще два каких-то исполняемых файла. Отметим, что именно такое поведение характерно для популярных последнее время троянов семейства Trojan.Downloader. Хеш-суммы загруженных файлов также помещаются в базу репутации файлов, а адреса, с которых производилась загрузка пополняют базу репутации сайтов. с Адреса, с которых загружаются дополнительные компоненты также помещаются в базу репутации сайтов.

Есть и более простые примеры использования корреляции. Например, если с серверов определенного провайдера рассылается подозрительно много спама, то и все сайты, которые размещены у данного провайдера получают низкую репутацию. Разумеется, что это не означает, что доступ к ним однозначно блокируется, но им оказывается более пристальное внимание.

Третьим способом определения репутации ресурсов в базах SPN является система обратной связи. Фактически SPN учитывает обращение клиентов Trned Micro к ней для ее собственного пополнения. Проще всего такой подход пояснить на примере репутации для электронной почты. При выявлении спам-письма, IP-адрес отправителя помещается в базу на относительно короткий срок (в пределах нескольких часов). Такой осторожный подход призван застраховать от блокировки легитимных источников почты, которые отправили что—то напоминающее спам. Если же в течение этих нескольких часов большое количество клиентов Trend Micro обратиться к базе репутации электронной почты, чтобы свериться относительно репутации данного адреса, то это явный признак того, что адрес попал с базу не случайно. При таком развитие событий адрес “прописывается” в базе на очень долгое время. Разумеется, что если все таки произошла ошибка, у любого пользователя всегда есть возможность удалить свой адрес из базы.

Если попытаться сформулировать суть SPN, то эта облачная инфраструктура позволяет отслеживать поведение вредоносных программ в масштабе всего интернета, а не непосредственно на компьютере жертвы. Это дает существенные преимущества перед современными угрозами, которые научились обманывать, как пользователя, так и защитное ПО, установленное у него на компьютере.

Использование фильра SmartScreen

Последней технологией безопасности, которую мы рассмотрим, использует огромное количество пользователей, это фильтр SmartScreen, встроенный в Internet Explorer, начиная с версии 8.

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

По статистике производителя, SmartScreen блокирует ежечасно более 125 тыс. потенциально небезопасных сайтов и программ.

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 файл со списком в несколько 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. Каждый пользователь обладает возможностью 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.

Выводы

Множество технологий движутся к использованию облачных инфраструктур. Навигаторы переходят на загрузку в реальном времени карт от Google, вместо прошитых в устройство при покупке. Мало кто заглядывает в энциклопедии в наше время, чаще сверяются с Wikipedia. Вот и защитные технологии не стоят в стороне от этого процесса.

Как было сказано в начале, многие пользователи если и слышали об облачных технологиях, то представляют их себе, как некую отдаленную перспективу развития информационных технологий. На самом деле оказывается, что такое привычное решение, как антивирус или интернет браузер на сегодняшний день не способно без использования облачных технологий обеспечить защиту пользователю.