15 Октября, 2009

Новая Эра в Сфере Безопасности

Необходимо найти совершенно новый подход к корпоративной безопасности и, что важнее всего, перенести защиту в облачную инфраструктуру. Это позволит получать максимальную отдачу от объединенной мощности компьютеров и увеличить эффективность и скорость реакции системы.

Николай Романов, технический консультант Trend Micro в России и СНГ

Природа угроз безопасности (впрочем, как и сама организованная преступность) значительно изменилась за последние годы, а средства защиты развиваются слишком медленно, чтобы дать достойный отпор современным атакам. И если разработчики будут все также делать упор на защиту конечных точек, то вся отрасль обречена на поражение в неравной борьбе со все более изощренными угрозами. Необходимо найти совершенно новый подход к корпоративной безопасности и, что важнее всего, перенести защиту в облачную инфраструктуру. Это позволит получать максимальную отдачу от объединенной мощности компьютеров и увеличить эффективность и скорость реакции системы.

На протяжении последних 10 лет характер угроз безопасности быстро менялся. Десять лет назад угрозы были статическими, исходили от непрофессиональных взломщиков, и защита от них также была относительно простой и состояла по большей части из сбора образцов вредоносного программного обеспечения, разработки шаблонов и их распространения по конечным точкам для распознавания вирусов. До 2001 года угрозы, включая вирусы, черви и троянские кони, получали широкую известность, как это было с компьютерными червями Melissa, CodeRed, Snapper и Spammer. Благодаря широкому освещению в средствах массовой информации эти угрозы было сравнительно легко распознавать с помощью средств безопасности, работающих на основе шаблонов.

Между 2001 и 2003 годами произошел резкий рост количества злоумышленников, массово рассылающих спам. Затем стали популярными программы-шпионы, после чего средства защиты от них были добавлены во все типовые системы безопасности. В 2005 году наступила эпоха интеллектуальных ботнетов, создававшихся путем заражения конечных точек вредоносными программами. Зараженные компьютеры начинали рассылать спам, выступать в роли хранилищ вредоносных программ или участвовать в проведении атак DDoS. Однако сканирования предположительно зараженных конечных точек по-прежнему было достаточно для выявления и нейтрализации вредоносных программ.

В середине 2007 года появился новый тип угроз, исходящих из Интернета. Новые атаки вредоносных программ отличались от всех своих предшественников сразу по нескольким параметрам. Правила игры изменились, и традиционные средства защиты уже неспособны устоять перед новым врагом.

Новые угрозы

Во-первых, угрозы, исходящие из Интернета, характеризуются наличием множества стадий и вариантов атак. Это означает, что на первый взгляд безобидное электронное сообщение может содержать ссылку, при щелчке на которой активируется программа загрузки, проверяющая через Интернет наличие уязвимостей и загружающая другие вредоносные программы: спамботы, боты DoS и другие вирусы. Многовариантные угрозы с трудом

распознаются при традиционном эвристическом шаблонном сканировании, потому что сначала они кажутся чем-то одним, но затем сами обновляются через Интернет и меняются со временем.

Во-вторых, угрозы, исходящие из Интернета, распределяют свою работу по множеству хостов. Любая из этих составляющих сама по себе может казаться безобидной, но при объединении всех частей образуется серьезная угроза. В-третьих, при организации угроз, исходящих из Интернета, используются различные протоколы, включая многоступенчатую загрузку данных по протоколу SMTP, HTTP и веб-систем обмена сообщениями. И в-четвертых, для реализации угроз используются сразу несколько технологий, блокировка которых требует применения многоуровневых систем защиты.

В то же время значительно изменились мотивы и организация киберпреступности, что привело к существенному усложнению отслеживания их деятельности. Век массовых атак закончился. Червь Worm_Downad (Conficker), заразивший в январе этого года миллионы компьютеров через уязвимую точку Microsoft RPC, был первым примером такой атаки за несколько лет. И это говорит не только об улучшении защиты, но и об изменении целей киберпреступников.

Сегодня главным стимулом для мошенников является финансовая выгода. Ради денег они контролируют компьютеры, выманивают банковскую информацию и пароли и, возможно, передают эту информацию другим лицам. Поэтому массовые атаки противоречат их целям: преступники не хотят быть пойманными, они хотят, чтобы их вообще не замечали.

Исследования показали, что подпольная компьютерная экономика резко пошла вверх с началом торговли уязвимостями, когда независимые бизнесмены нанимают поставщиков вредоносного программного обеспечения и, пользуясь средствами, скрывающими их операции, занимаются мошеннической деятельностью. Для распространения своего смертоносного оружия они нанимают поставщиков ботнетов и хакеров. Цены на черном рынке на удивление доступные. Всего за 100 долларов в день можно купить атаку DDoS, а за 1 000 долларов можно купить 10 000 зараженных компьютеров.

При этом по данным сайта AV-Test.org рост количества вредоносных атак феноменален: от 1 738 отдельных случаев в 1988 году до 5,7 миллиона только за первые 6 месяцев прошлого года. В настоящее время регистрируется около 800 угроз в час, и их число продолжает расти. По прогнозам, к 2015 году это число может вырасти до 26 500 атак в час.

Новые задачи

Изменение природы атак и феноменальный рост их количества создают значительное поле для деятельности разработчиков средств защиты. Но индустрия средств безопасности почти не изменилась с момента разработки первых стандартных решений более 10 лет назад. Сейчас традиционное обновление шаблонов вредоносных программ стало проводиться гораздо чаще: уже не раз в неделю, а раз в час или даже полчаса, но по сути принцип остался неизменным: собрать образцы вирусов и быстро распространить их по конечным точкам. Но поскольку изменился характер угроз и злоумышленники стараются сделать свою деятельность незамеченной, сейчас становится особенно трудно найти прошлые аналоги новых атак.

Киберпреступники также становятся все более искушенными в создании разнообразных вариантов вредоносных программ с различными механизмами доставки. Это означает, во-первых, что значительно возрастет размер файлов с шаблонами для поиска сигнатур, а значит, вырастут требования к дисковому пространству, объему памяти и вычислительной мощности конечной точки. Во-вторых, обновление таких файлов будет занимать больше времени и создавать высочайшую нагрузку на сеть. Но что самое плохое, даже если эти файлы с шаблонами удастся установить, их обновление и анализ данных будут требовать

такого количества ресурсов, что компьютеры будут буквально замирать и прекращать выполнение всех прочих задач.

Если мы не пересмотрим методы защиты конечных точек, то к 2015 году развертывание систем защиты в крупных организациях станет просто нецелесообразным. На обновление одного файла шаблонов в компании с 250 000 сотрудниками по всему миру может потребоваться более 5 часов, что вряд ли можно назвать быстрым ответом на критически опасную угрозу для бизнеса. А если компании будут получать обновления до 8 раз в день и предварительно тестировать файлы шаблонов в контролируемой среде (как это делается в некоторых организациях) до развертывания в корпоративной сети, то идея постоянной готовности к атакам станет недостижимой. Сетевые администраторы будут тратить все свое время на управление обновлениями, сети будут постоянно перегружены непрерывной загрузкой обновлений, и производительность конечных точек будет поставлена под вопрос. Что уж тут говорить об удаленных и мобильных сотрудниках, которые смогут получать обновления только через несколько дней после их выпуска.

Совершенно ясно, что требуется новый подход, который позволит получать максимальную отдачу от современных технологий и ресурсов. Ответ лежит в идее переноса бремени хранения и средств обнаружения угроз в облачную инфраструктуру. Это позволит до минимума сократить нагрузку на конечные точки и сеть, а также мгновенно обнаруживать новые атаки и блокировать угрозы. Это подход можно назвать гибридным, потому что некоторые угрозы будут обнаруживаться при проходе через шлюзы по подозрительным IP-адресам или блокированным отправителям, а некоторые — локально путем распознавания сигнатур. И хотя мы говорим об облачной инфраструктуре, крупные корпорации также будут хранить локальные копии базы данных угроз, чтобы максимально ускорить скорость ответа системы на обращения клиентов.

Система безопасности в действии

Инфраструктура Trend Micro Smart Protection Network, работающая по схеме «облако-клиент», разработана специально для таких случаев и состоит из трех компонентов: технологии оценки репутации почты, сайтов и файлов; функции сопоставления событий и функции обратной связи с пользователем. В этой инфраструктуре поддерживается глобальная сеть хранилищ информации об угрозах, применяемая для анализа более чем 50 миллионов подозрительных IP-адресов и адресов URL в сутки. Данная инфраструктура обрабатывает более 5 миллиардов запросов в день и обеспечивает всестороннюю защиту от всех типов угроз, включая новейшие угрозы из Интернета.

Комбинация этих трех компонентов делает Smart Protection Network прекрасным решением для обнаружения угроз, поскольку появляется возможность анализировать взаимосвязь между различными событиями. Примером такого события может быть резкое увеличение количества спама с одной и той же подозрительной ссылкой, по которой загружается программный код, через некоторое время становящийся вредоносным. В таких случаях функция сопоставления событий позволяет получить цельную картину ситуации и повысить качество информации в базе данных угроз.

В инфраструктуре Smart Protection Network также применяется функция глобальной обратной связи, помогающая выявлять источники угроз и обеспечивающая взаимосвязь между исследовательскими центрами, пользователями, продуктами и услугами. Поэтому если, например, в сообщении электронной почты содержится подозрительная ссылка на вредоносный код, это сообщение будет мгновенно блокировано в локальном шлюзе, адрес сайта будет добавлен в черный список, база данных репутации сайтов будет обновлена и шаблон файла будет загружен в базу данных репутации файлов.

Smart Protection Network иногда сравнивают с электронной версией добровольной народной дружины, когда соседи постоянно заботятся друг о друге и предотвращают беду до ее

появления. Дни, когда для отпугивания преступников по каждой улице ходил полицейский со свистком, ушли в прошлое. Инфраструктура Smart Protection Network олицетворяет новый подход, позволяющий использовать все преимущества новейших технологий, в то время как методы защиты предыдущего поколения уже исчерпали себя, а ведь дальше будет становиться только сложнее.