Глубокий анализ трафика как шаг к безопасному Интернету

Юрий СЕНЧЕНКО,
к.т.н., руководитель направления «Широкополосные системы» ООО «НТЦ ПРОТЕЙ»

Расширение пространства борьбы

Согласно статистической оценке Международного союза электросвязи по итогам 2011 года, количество пользователей сети Интернет за последние пять лет удвоилось и превысило 2,4 млрд человек, что свидетельствует о ее продолжающемся интенсивном росте. Подобное разрастание ожидаемо сопровождается усилением влияния Интернета на самые разные аспекты современного общества: преимущества от интеграции в глобальную сеть являются сегодня столь существенными, что пренебречь ими — значит заведомо проиграть на любом конкурентном поле. Известно, однако, что увеличение значимости продукта технического прогресса, как правило, сопровождается столь же масштабным негативным эффектом в случае его некорректной работы (вспомним поломку водопровода или забастовку сотрудников авиакомпании). К большому сожалению, Интернет не стал исключением, а подтвердил это правило на 100%, и с ростом зависимости общества от глобальной сети последствия ее беспечного использования становятся все опаснее. Раскрытие коммерческой тайны, кража средств с банковской карты, падение важного ресурса под воздействием атаки — обычные в наши дни явления, приносящие многомиллионные убытки корпоративным и частным пользователям. Последствия некоторых интернет-атак, таких как хищение учетной записи электронной почты или социальной сети, доступ малолетних детей к информации «только для взрослых» или несанкционированное подключение к web-камере домашнего компьютера не поддаются монетарной оценке, однако могут нанести гораздо более существенный ущерб по сравнению с финансовыми потерями.

Вероятность оказаться жертвой упоминаемых атак существовала на протяжении всей истории развития глобальной сети — создавались и механизмы ее снижения. Однако сегодня развитие технологий, многообразие услуг, а также, как это ни удивительно, повышение уровня компьютерной грамотности пользователей приводят к тому, что найденные ранее методы обеспечения сетевой безопасности становятся неэффективными. Как следствие, возникает необходимость применения новых решений, учитывающих изменчивую природу глобальной сети и использующих комплексный многоуровневый подход.

Состояние вопроса

В силу того что интернет-атаки направлены как на отдельных пользователей, так и на организованные группы (предприятие, школа, университет), имеет смысл выделить индивидуальные и групповые механизмы контроля вредоносного трафика.

Наиболее распространенным на сегодня способом ограничения доступа к опасному контенту являются устанавливаемые на ПК индивидуальные антивирусные программы. Применение подобных программ — достаточно эффективная мера противодействия интернет-угрозам: антивирусы блокируют доступ к сайтам с сомнительной репутацией, имеют обновляемую базу вредоносного ПО, а также позволяют ограничить доступ детей к нежелательным ресурсам.

К недостаткам антивирусных пакетов можно отнести использование вычислительных ресурсов компьютера, а также необходимость обновления антивирусного ПО. Пользователи, сталкивающиеся с нехваткой производительности, часто считают (и иногда небезосновательно), что причиной медленной работы является антивирусная программа. В итоге, желающие быстрее получить доступ к любимым интернет-ресурсам пользователи временно отключают ее, разом лишаясь всего арсенала средств борьбы с сетевыми угрозами. Необходимость устанавливать регулярные обновления также увеличивает риск заражения. Если пользователь игнорирует уведомление программы о необходимости скачать новую версию антивирусных баз, он может стать жертвой атаки, разработанной после последнего обновления продукта. Наконец, антивирусное ПО необходимо покупать, инсталлировать и периодически оплачивать продление лицензий. В результате, безопасность пользователя зависит от ответственности

самого пользователя, то есть того самого «человеческого фактора».

С точки зрения ответственности ситуация отличается в лучшую сторону в сегменте защиты компьютеров, объединенных в учрежденческую сеть. Во-первых, за обновлением антивирусных пакетов в таких сетях следят уже не сами пользователи, а назначаемые ответственные лица — сетевые администраторы. Во-вторых, для учрежденческой сети выход в Интернет обычно настраивается через единую точку — прокси-сервер, который разрешает использовать строго определенные порты, а также закрывает доступ к заранее внесенным в черный список ресурсам, например к развлекательным сайтам. Учрежденческий прокси-сервер также может быть интегрирован с антивирусным пакетом, что позволяет распространить его действие сразу на всю сеть. Перечисленные способы защиты «закрывают» часть задач по обеспечению сетевой безопасности, однако и этого, как правило, оказывается недостаточно, так как учрежденческая сеть предъявляет гораздо более строгие требования к контролю трафика, нежели обычный домашний компьютер.

В качестве примера достаточно упомянуть наболевшую проблему администраторов практически всех сетей: закрытие доступа к нежелательным (преимущественно развлекательным) ресурсам. Сложность этой задачи возрастает с ростом компьютерной грамотности пользователей и появлением программного обеспечения, предназначенного для обхода фильтров. Использование неконтролируемых интернет-прокси, работающих, в том числе, и по шифрованному соединению, практически сводит на нет усилия сетевых администраторов. Наряду с этим современные программы файлового обмена позволяют обойти защиту путем использования стандартных портов, закрытие которых невозможно, так как повлечет ограничение доступа ко всей внешней сети. В результате, единственным относительно действенным механизмом предотвращения нецелевого использования является ограничение доступного для скачивания объема данных. Этот проверенный метод обладает очевидным недостатком: при необходимости доступа к материалам, действительно требуемым для работы, в то время как выделенный трафик уже израсходован, администратору сети приходится открывать дополнительные разовые квоты, что в рамках более-менее крупной сети является изнурительной задачей. Помимо этого, необходимость формального запроса к администратору является преградой, замедляющей организационные процессы компании — как результат, вместо ожидаемого положительного эффекта сетевая безопасность чинит препятствия нормальному функционированию компании.

Следует также упомянуть, что привлечение квалифицированного администратора и закупка пакетов антивирусного ПО требуют выделения бюджета, размер которого разрастается пропорционально количеству и размеру контролируемых сетей. В условиях кризиса (по опыту последних лет — перманентного состояния экономики), когда бюджета зачастую не хватает даже на первичные нужды, финансирование сетевой безопасности, к сожалению, часто отодвигается на второй план.

Централизация и глубокий анализ трафика

Логичным этапом эволюции механизмов ограничения доступа к нежелательному контенту является перенос функций контроля трафика еще на один уровень выше: из учрежденческих сетей в ядро сети оператора. Размещение оборудования в операторской сети (рис. 1) позволяет не только преодолеть ограничения двух предыдущих подходов, но и существенно расширить арсенал средств борьбы с сетевыми злоумышленниками. Рассматривая централизованное решение в контексте описанных особенностей известных методов контроля трафика, можно заключить, что:

а) все задачи по обновлению антивирусных баз, категорий сайтов и пр. концентрируются в ядре сети — исключается воздействие «человеческого фактора»;

б) операторское решение предоставляет учрежденческим сетям более широкий набор функций при меньших затратах за счет экономии на масштабах и централизации;

в) по сравнению с локальными решениями централизованное решение, как правило, оснащено более мощным инструментарием контроля трафика.

Остановимся чуть более подробно на последнем пункте.

Локальные решения в большинстве своем неспособны блокировать трафик приложений, позволяющих обойти защитные механизмы сети. Решения операторского класса, напротив, представляют собой высокопроизводительные анализаторы, детектирующие тип передаваемого или получаемого контента даже в шифрованном потоке данных посредством применения вероятностных механизмов анализа. В частности, решение НТЦ ПРОТЕЙ среди

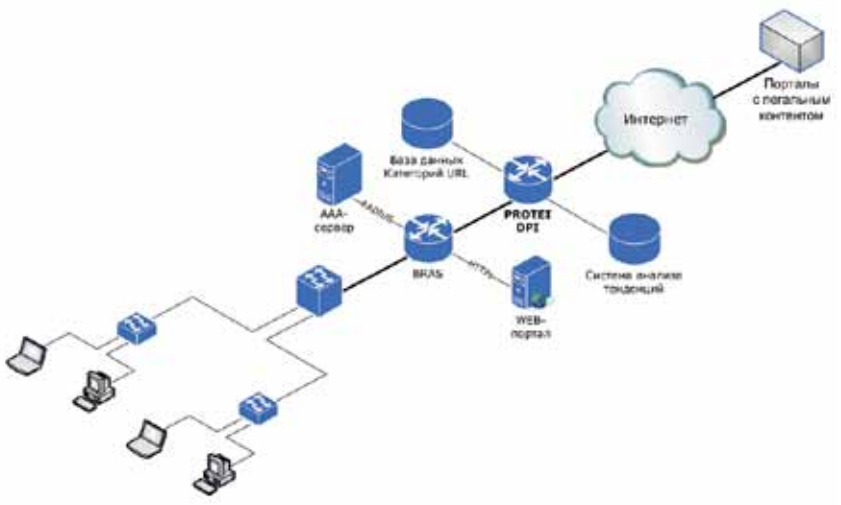

Рис. 1. Система глубокого анализа трафика в сети оператора ШПД

других методов распознавания использует статистические критерии, а также поведенческие детекторы. Подобный инструментарий позволяет преодолеть защиту от блокирования, применяемую сегодня широким спектром сетевых приложений, и таким образом ограничить доступ даже опытных пользователей к нежелательному контенту.

Блокирование интернет-прокси, открывающих доступ к сайтам из запрещенного списка, при централизованном решении осуществляется с большим эффектом за счет комбинирования возможностей системы глубокого анализа трафика и базы категорий URL, обновляемой в реальном времени. Анализ содержимого потоков данных, в том числе и шифрованного трафика, также позволяет распознавать и блокировать трафик к настраиваемым в браузерах удаленным проксирующим серверам.

Применение программно-аппаратных комплексов глубокого анализа трафика, помимо высокоточного детектирования протоколов, предоставляет возможность решения целого спектра приоритетных задач, в числе которых:

1. Блокирование вредоносного трафика DoS, DDoS, SPAM-рассылок, сканирования сети. Защита учрежденческих сетей от атак типа «отказ в обслуживании» эффективнее выполняется на уровне ядра сети оператора. Предотвращение отказа стратегических ресурсов под воздействием распределенной атаки является ключевой задачей в условиях зависимости функционирования структур от доступности удаленных систем. Ограничение несанкционированных почтовых рассылок, а также блокирование сканирования сетей обеспечивает дополнительную безопасность пользователей, предотвращая распространение вредоносного ПО.

2. Централизованный контроль сайтов, оперативное управление доступом к информации. Независимые распределенные системы защиты учрежденческих сетей не позволяют оперативно реагировать на появление сайтов, содержащих недопустимые материалы и вредоносное ПО. Это обусловлено тем, что обновление черных списков ресурсов и антивирусных баз требует раздельного управления настройками на распределенных объектах, что труднее осуществить единовременно. Известно, однако, что вредоносные материалы имеют свойство распространяться лавинообразно, поэтому критически важно отследить их появление на самых ранних этапах. Необходимость по возможности более скорого пресечения доступа объясняется также тем, что технически подкованные пользователи, которых сегодня много даже среди учащихся шестых-восьмых классов школ (что само по себе довольно отрадно), могут, получив хотя бы кратковременный доступ к ресурсу, сохранить его и начать распространять посредством файлообменных сетей. В отличие от распределенной системы, централизованная точка применения правил, синхронизированная с базой категорий ресурсов, позволяет мгновенно внести в черный список вредоносные сайты. Возможность контроля трафика файлообменных сетей ограничивает дальнейшие пути его распространения.

3. Увеличение доли легального контента. В силу того что централизованное решение анализа пакетов дает возможность блокировать трафик файлообменных сетей, операторы могут ограничивать распространение нелицензионного контента, тем самым предотвращая эпизоды нарушения авторских прав. В то же время возможность перенаправления потоков данных позволяет указать абонентам источники лицензионного контента, в продвижении которого в последнее время все чаще участвуют операторы.

Относительно неподробному описанию возможностей централизованного решения по управлению пакетным трафиком можно с легкостью посвятить целую серию публикаций. В рамках настоящей статьи обозначены лишь основные моменты, которые, по мнению автора, заслуживают внимания при выборе подходов к обеспечению сетевой безопасности. В то же время усиливающаяся напряженность на просторах глобальной сети сформировала как со стороны обычных пользователей, так и со стороны государства отчетливый спрос на хотя бы минимальный контроль практически неуправляемого сегодня Интернета. Одним из наиболее эффективных инструментов обеспечения подобного контроля можно с уверенностью назвать системы глубокого анализа трафика.